The Auditor-General
ANAO Report No.29 2017–18
Performance Audit

Unscheduled Taxation System Outages

Australian Taxation Office

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-326-3 (Print)
ISBN 978-1-76033-327-0 (Online)

Senior Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
communication@anao.gov.au.

Australian National
Audit Office

Canberra ACT

20 February 2018

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Australian Taxation Office titled *Unscheduled Taxation System Outages.* The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website—http://www.anao.gov.au.

Yours sincerely

Grant Hehir

Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Fax: (02) 6203 7777
Email: ag1@anao.gov.au

ANAO reports and information about the ANAO are available on our website:
http://www.anao.gov.au

Audit team

Alex Doyle
Mark Harradine
Judy Jensen
Alison Millea
Steven Favell
Andrew Morris

Contents

Summary and recommendations

Background

1. The Australian Taxation Office (ATO) relies on information, communications and technology (ICT) systems to conduct its business, and online services have become the primary means of transacting with the ATO. It is important that the ATO's ICT systems are accessible, as there are few or no practical alternatives to doing business when these systems and services are unavailable.

2. Over the past year, the ATO has experienced a number of failures in system components that have led to system failures and unscheduled outages in its online services. The most significant system failures occurred in December 2016 and February 2017, and were caused by problems with the data storage area network.[1] In June 2017, the ATO released a report into these two system failures. Based on post incident reviews, the *ATO systems report* outlined the causes of the system failures and impacts on stakeholders, analysed the ATO responses and provided recommendations for more resilient and accessible systems and services in the future.

Audit approach

3. The objective of the audit was to assess whether the Australian Taxation Office has effectively responded to recent system failures and unscheduled outages.

4. The high-level criteria were that the ATO:

- effectively responded to the particular system failures and outages;
- revised its information, communications and technology (ICT) governance, systems and processes in line with the agreed recommendations in the post incident reviews of the system failures; and
- has established and met service commitments and outage tolerances for ICT system availability.

Conclusion

5. The ATO's responses to the system failures and unscheduled outages were largely effective, despite inadequacies in business continuity management planning relating to critical infrastructure. The post-incident reviews commissioned and conducted by the ATO have informed the ongoing management of its ICT environment, including through strategies and actions to improve ICT governance, strengthen business continuity processes and address availability and resilience gaps in systems infrastructure.

6. The ATO has structured its response to the system failures of December 2016 and February 2017 around the 14 recommendations included in the *ATO systems report*. The ANAO considers that, at November 2017, the ATO had implemented four recommendations and partly implemented the remaining 10 recommendations. The implemented recommendations mainly

[1] A storage area network is a dedicated high-speed network that interconnects shared pools of storage devices to multiple servers.

relate to technical solutions to the particular system failures, while the broader initiatives to strengthen ICT governance and processes are underway. Considerable work is required to implement the recommendations before many of the intended and agreed outcomes are achieved.

7. The ATO does not have service commitments specifically relating to the availability of ICT systems but does specify system outage tolerances in its major contracts with ICT service providers. To monitor the impact of ICT service outages on satisfaction with its services, the ATO should develop service standards that are aligned with system outage tolerances in its contracts with ICT service providers.

Supporting findings

Responding to system failures

8. In response to the incidents in December 2016 and February 2017, the ATO invoked its business continuity management plan, but the plan included limited actions to correct ICT system failures associated with critical infrastructure including data centres. The business continuity processes also did not recognise weaknesses in ICT design—particularly that the system recovery tools used to restore ICT services were on the affected storage area networks—which resulted in services not being fully restored for ten days for the December 2016 incident and five days for the February 2017 incident. Despite limited planning for critical infrastructure failure, the ATO's responses to the incidents were largely effective, as it worked closely with the contracted ICT service providers to identify the system fault and restore services in line with activation guidelines, but could have better communicated with stakeholders throughout the incidents.

9. The ATO undertook extensive investigation into the system failures to understand their cause and inform the ongoing management of its broader ICT environment. The ATO commissioned key reviews into the system failures that resulted in eight reports on the cause and response to the failures, ICT governance, and the extent of availability and resilience gaps in the ICT environment. A major outcome of the reviews was the identification of 14 key areas for improvement that fall into five general themes: principles informing the ATO's ICT design; correcting the identified system faults; enhancing ATO capability to support infrastructure design and ICT governance; incident responses for the ATO and the wider tax system; and managing communications and business resumptions with stakeholders.

Initiatives to reduce system failures

10. The ATO has examined its ICT infrastructure to identify availability and resilience gaps, and has reviewed and updated its IT Program of Work and associated projects to focus on improving availability and resilience, particularly for the more important applications. The reviews have identified that further work is required to improve system design and deliver corporate objectives. At the time of audit fieldwork, there were no target dates or milestones for completing this work or implementing the two recommendations in this theme.

11. A new storage strategy was approved, and the failed storage area networks were replaced and independently certified for use in readiness for Tax Time 2017. Control systems used to manage data, monitor systems and restore services are now hosted on separate infrastructure. The implementation of the new IT Systems Improvement Program has improved

resilience to system failures for most services, although further planned initiatives remain a work in progress. This recommendation is being implemented, and the other three recommendations in this theme have been implemented.

12. The ATO has implemented several initiatives to enhance systems capability and resilience, including accelerating the use of cloud computing services and in-house oversight on infrastructure architecture. Activities are underway to implement active monitoring systems and centralised logging of transactional events across the infrastructure—this recommendation is being implemented, as are the other two recommendations from this theme.

13. The ATO has reviewed its business continuity framework and identified areas for improvement, with updates to key BCM artefacts including the BCM Team Plan and a *Practical guide to Business Continuity in the ATO*. Further activities are underway to mature the ICT incident management, communication and escalation workflow to better reflect effective planning and response to ICT-related incidents. Forums have been held with superannuation and tax agents to assist them in improving their own business continuity strategies to help improve the resilience of the entire tax and superannuation system. All three recommendations in this theme are being implemented.

14. The ATO has updated its communication strategy with a greater focus on providing relevant and useful information to internal and external stakeholders, using multiple channels, during system failures and unscheduled outages. The ATO has examined options to clearly communicate information about the application of general waivers and discretions in particular circumstances but has not resolved an approach—this recommendation is being implemented, and the other recommendation from this theme has been implemented.

Service commitments and outage tolerances

15. The ATO does not have clear service commitments relating to the availability of ICT systems. There are no explicit measures for ICT service availability and existing service commitments have only broad application—through survey questions about ease of accessing services and information, and doing business with the ATO, and measures of timeliness in processing lodgements. Accordingly, the ATO has not broadly monitored the impact of ICT service outages on satisfaction with its services.

16. Outage tolerances are included as service measures in service level agreements for the major ICT service contracts, and equate to high availability of services and systems. Tolerances have been internally reported as largely met in recent years, although the recent system failures have been excluded, which means performance has been overstated for 2016–17. With the major ICT service contracts scheduled to be renegotiated in 2018, the ATO has an opportunity to align service measures across its ICT contracts and also align service standards with the outage tolerances in its ICT service contracts.

Recommendations

Recommendation no.1
Paragraph 2.10

The ATO updates its Business Continuity Management, IT Service Continuity Management and Risk Management frameworks to improve and better integrate the identification and treatment of risks to critical infrastructure that may lead to system failures.

Australian Taxation Office response: *Agreed.*

Recommendation no.2
Paragraph 4.12

The ATO determines the level of availability of services associated with ICT systems to include in service standard(s) and subsequently reports performance against those standard(s).

Australian Taxation Office response: *Agreed.*

Recommendation no.3
Paragraph 4.29

The ATO includes tolerances in its ICT service contracts that align with service standards associated with ICT systems, where possible.

Australian Taxation Office response: *Agreed.*

Summary of Australian Taxation Office response

17. The Australian Taxation Office's response to the proposed report is provided below and at Appendix 1.

> The ATO welcomes this review and considers the report supportive of our overall approach to managing our IT environment since the outages occurred in December 2016 and February 2017. The review complements the ATO and other independent reviews undertaken to date, and acknowledges the ATO's commitment and progress to improving the availability and resilience of our IT systems. As indicated in the ATO Systems Report published in June 2017, the system outages that we experienced in late 2016 and early 2017 were unexpected and to our knowledge unprecedented.
>
> As acknowledged by the review, the ATO's responses to the outages have been largely effective and we have been committed to understanding the cause of the failures and applying these insights to enhance the services we provide to the community.
>
> We have learnt from our experiences and have made many improvements to strengthen our systems. We have also improved our governance and business continuity management processes, as well as implemented improved monitoring. We will continue to work with our vendors and digital service providers to develop joint continuity plans.
>
> This report identifies that, as at November 2017, the ATO had implemented 4 of the 14 recommendations identified in the ATO Systems Report, with the remaining 10 recommendations still in the process of being implemented. We can now report that 9 of the 14 recommendations have been fully implemented. The remaining five recommendations will be completed throughout this year.
>
> The report also notes that the ATO engaged PwC to more broadly investigate the resilience of the ATO's ICT infrastructure in April 2017. This review was part of our long-term resilience program, and was aimed at identifying future investment priorities for the ATO to best ensure minimal disruption to services should the ATO ever experience further outages of the nature experienced in December 2016 and February 2017. The resilience risks identified by PwC as part of that review

and discussed in this report do not relate to the likelihood of another infrastructure failure occurring, but rather what the likely impact would be on ATO services if such an event was to occur. An IT Systems Improvement Program is currently underway, and will continue over the next few years, to address the priority investment areas identified in this review.

In relation to service commitments that we will identify for the availability of services associated with ICT systems, as contemplated by recommendation 2 in the report, our intention is that we will manage the consequences associated with our performance against these commitments in the same way we do for our current service commitments. A range of existing mechanisms (such as Parliamentary scrutiny) already exist to hold the ATO accountable for performance against our service commitments, and we consider these mechanisms would be equally applicable in this case.

The ATO agrees with the three recommendations contained in the report.

Key learnings for improvement for all Australian Government entities

18. Below is a summary of key learnings and areas of good practice identified in this audit report that may be considered by other Commonwealth entities when managing enterprise ICT systems.

Governance and risk management

Governance arrangements

- With the increasing reliance on contracted ICT service providers to deliver services, entities should review their ICT governance arrangements to:
  - monitor the performance of systems, ideally with active monitoring systems;
  - assess the delivery of contracted services using reliable data;
  - establish ICT procurement guidelines to accommodate a changing digital environment, including the transition towards new technology and service providers; and
  - ensure that the entity, as the service integrator, provides effective oversight and control of the outsourced environment.

Business continuity processes

- Conduct a comprehensive business impact analysis to identify business processes that are critical to continued service operation; design risk treatments to identify and mitigate the risks of system failures; and periodically test the risk treatments.
- Store system recovery tools used to restore ICT services across multiple systems.
- In response to major system failures, conduct extensive reviews and establish a clear and timely program of work to improve the management of the ICT environment.

Service commitments

- Define service commitments for online services, including the availability of ICT systems, and specify equivalent maximum acceptable system outage tolerances in ICT service contracts.

Audit findings

1. Background

Introduction

1.1 The Government released the National Digital Economy Strategy[2] in May 2011. The strategy notes that effective government participation in the digital economy can reduce costs, increase individuals' satisfaction and promote innovation. Participation also makes it easier for government to facilitate online engagement and collaboration, improve service delivery and contribute to policy and regulatory matters.

1.2 The Digital Transformation Agency notes that 'Australians are more mobile, more connected and more reliant on technology than ever before' and government is responding through improvements in online service delivery.[3] Major disruptions to online services in this environment can have major consequences for government agencies and the people dealing with them.

1.3 According to the Australian Taxation Office (ATO), it contributes to the economic and social wellbeing of Australians by fostering willing participation in the tax and superannuation systems. It recognises the value of delivering digital government services, not only to the community in making it easier to meet their obligations, but to government in benefits realisation and responsible use of public monies.[4]

Digital transformation of the Australian Taxation Office

1.4 The Commissioner of Taxation is responsible for administering Australia's tax system and significant aspects of Australia's superannuation system, and operates as the Australian Government's principal revenue collection agency.[5] Responsibilities of the ATO include:

- collecting taxation revenue, such as personal income and company taxes;
- administering the goods and services tax on behalf of the Australian states and territories;
- administering a range of programs that result in transfers and benefits back to the community;
- administering major parts of Australia's superannuation system; and
- administering the Australian Business Register.

[2] Australian Government Information Management Office, *Australian Public Service Information and Communications Technology Strategy 2012-2015*, Department of Finance and Deregulation, 2015.

[3] Digital Transformation Agency, available from <https://www.dta.gov.au/what-we-do/> [accessed 25 August 2017].

[4] Senate Finance and Public Administration Committees, Australian Parliament, *Inquiry into digital delivery of government services* (September 2017), p. 3.

[5] Australian Taxation Office, *Commissioner of Taxation Annual Report 2016–17*, ATO, 2017, p. 4.

1.5 These responsibilities require interaction with a wide range of stakeholders including individual taxpayers (10.9 million), small businesses (3.8 million) and self-managed super funds (597 250). The ATO encourages taxpayers and other users to transact with it and obtain guidance through online channels. According to the ATO:

> We are enhancing and promoting our online transaction and tax guidance services. While the take-up of digital services is largely driven by demand for services that are accessible, secure, easy to use and always available, it also contributes to the efficient administration of the systems in the interest of the community as a whole.[6]

1.6 The ATO provides a range of online services, including those outlined in Table 1.1.

Table 1.1: Online services provided by the ATO

Online service	Intended stakeholder	Key functions of the service
ATO website	Taxpayers and tax agents, the superannuation industry and contributors and a variety of other external stakeholders.	Entry portal—provides access to other online services, a channel for some queries and a broad range of information.
myTax, accessed through myGov	Individuals and sole traders.	Lodge tax returns and other forms, maintain personal information, view assessments and personal account balance and transactions.
Business Portal	Businesses with an Australian Business Number (ABN).	Lodge activity statements, other online forms and objections. Request rulings. Update business registration details.
Standard Business Reporting	Businesses with an ABN and registered tax agents.	Automated upload of business accounting and other information.
Practitioner Lodgement Service/ Electronic Lodgement Services	Tax agents.	Lodgement of tax returns.
Tax Agent Portal	Tax agents.	Manage client details, communicate securely with the ATO and obtain client information.
BAS Agent Portal	Registered Business Activity Statement agents.	Manage client details, communicate securely with the ATO and obtain client information.
Small business superannuation clearing house	Employers with 19 or fewer employees, or with an annual aggregated turnover of less than $10 million.	Payment of superannuation contributions.
Australian Business Register	Businesses and tax professionals, public access to some details.	Issue ABN and Tax File Number, maintain and register business details, issue AusKEY.

Source: ANAO analysis of ATO information.

[6] Australian Taxation Office, *Annual Report 2015–16*, Volume 1, p. 15.

1.7 Use of online services is increasing, and these have become the primary means of transacting with the ATO, especially for lodging tax returns. According to the ATO, the ATO Tax Time 2017 has exceeded any prior year for electronic lodgement of tax returns (refer paragraph 3.11). The ATO also indicates that it is aligning with broader government directions for digital transformation. As stated in the 2016–17 Corporate Plan:

> Increasingly, our digital infrastructure and contemporary services allow us to engage with clients, our key stakeholders and each other in an online and mobile environment. We are part of, and will strongly support, the government's digital services agenda, including through the Digital Transformation Office in the Prime Minister and Cabinet portfolio.[7]

1.8 All services that were designed or redesigned after 6 May 2016 are within the scope of the Digital Service Standard[8], as issued by the Digital Transformation Agency. The standard includes a requirement to measure performance, with measures to be reported in an online dashboard on the Digital Transformation Agency's website. The Digital Service Standard states:

> Every service must aim for continuous improvement. Metrics are an important starting point for discussions about a service's strengths and weaknesses. By identifying and capturing the right metrics - with the right tools - you can make sure all your decisions to improve the service are supported by data.[9]

1.9 The Standard requires agencies to measure four key performance indicators at a minimum:

- *User satisfaction*—to help continually improve the user experience of your service;
- *Digital take-up*—to show how many people are using the service and to help encourage users to choose the digital service;
- *Completion rate*—to show which parts of the service you need to fix; and
- *Cost per transaction*—to make your service more cost efficient.[10]

Information and communications technology management arrangements of the Australian Taxation Office

1.10 The ATO's online services are the public facing element of its information and communications technology (ICT) architecture, managed primarily through a number of 'bundled' service contracts with contracted ICT service providers. These contracts were established in 2009 and 2010, replacing a single comprehensive contract for ICT infrastructure services (discussed in Chapter 4). The service bundles offered to the market were defined in an ICT Sourcing Strategy that aimed to support the ATO's business directions beyond 2010. Originally established for periods of five years, these contracts have been extended until 2018.

1.11 A summary of the ATO's ICT management arrangements with contracted ICT service providers is presented in Table 1.2.

[7] Australian Taxation Office, *ATO Corporate plan 2016–17*, p. 7. Available from <https://www.ato.gov.au/about-ato/about-us/in-detail/strategic-direction/ATO-corporate-plan-2016-17/> [accessed 6 October 2017].

[8] Digital Services Standard, available from <https://www.dta.gov.au/standard/> [accessed 21 September 2017].

[9] Performance measures in the Digital Service Standards, available from <https://www.dta.gov.au/standard/11-measure-performance> [accessed 20 September 2017].

[10] ibid.

Table 1.2: Summary of the ATO's ICT management arrangements with contracted ICT service providers

Contract	Service and assets required	Contracted ICT service provider	Contracted value ($ millions)
Managed Network Services	Carriage, phone/PABX, network, call centre infrastructure and security.	This was awarded to Optus, and the contract signed on 16 June 2009.	Approximately $60 million per year.
End-user Computing	The End-user Computing bundle contains two contracts: • one for the administration of the Enterprise Service Management Centre, including the conduct of problem management; and • the other for End User Technology and Support, including desktop, standard operating environment, service management and integration, service desk and security.	These were awarded to Lockheed Martin Australia, and the contracts signed on 10 September 2010. In August 2016, Lockheed Martin Australia was incorporated as Leidos.[a]	Approximately $45 million per year.
Centralised Computing	Midrange, mainframe, storage, data warehouse and security.	This was awarded to HP Enterprise (HPE), with the contract signed on 17 December 2010. In April 2017, HPE merged with CSC Australia (CSC), and became DXC Technology (DXC).[b]	Approximately $160 million per year.

Note a: Lockheed Martin's Information Systems & Global Solutions business was sold globally to Leidos in August 2016. Datacom is its support partner in the delivery of desktop outsourcing services for the ATO.

Note b: CSC and the Enterprise Services business of HPE completed their merger in April 2017. Accordingly, the company will be referred to as DXC in this audit report, unless a particular report or event was specifically linked to HPE.

Source: ANAO analysis based on data from ATO's contracts with the contracted service providers.

1.12 The scope of these contracts is comprehensive. The ATO has in effect fully outsourced ICT infrastructure functions. In this environment the ATO retains responsibility for ICT services, but they are performed and managed by the contracted ICT service providers.

1.13 Oversight and control of ICT vendor activities is framed by the contracts with each contracted ICT service provider and the associated service level agreements. These agreements establish performance standards. They also set out the way in which the parties will communicate with each other—when, how and in respect of what matters. The contracts cover periods of normal operations and responses to events that threaten to, or actually, severely degrade a system's availability and performance.

1.14 The ATO has characterised the relationship with DXC Technology (DXC) as a 'turnkey' solution—indicating that DXC is to provide a full infrastructure service with no routine input from the ATO. Leidos operates a digital dashboard—supported by visual analysis tools—over ATO's ICT systems, and provides a problem management process should issues arise with parts of the infrastructure.[11]

1.15 The role of the ATO as the service integrator—in providing oversight and control in an outsourced environment—is vital to the continuity and standard of ICT services. The obligations of contracted ICT service providers are defined by the terms of the contracts. No matter how well contracts are specified and enacted, there will always be a need for attentive oversight. Matters such as overall systems design, scope of functions and user interaction cannot be fully divested from an agency. In an environment where multiple vendors provide services, service integration is a key matter.

System failures

1.16 Over the past year, the ATO has experienced a number of problems within its enterprise ICT systems that have led to system failures and unscheduled outages in online services. These system failures have occurred due to failures in system components. A summary of the system failures that affected online ATO services in late 2016 and 2017 are presented in Table 1.3.

Table 1.3: Summary of ATO system failures in late 2016 and 2017

Start date of the system outage	Duration of the outage	Services affected	Cause of the outage and delay to restore services
12 December 2016	10 days	All ATO systems	• Storage area network hardware failure. • Inadequate monitoring. • Recovery tools stored on failed storage area network.
2 February 2017	5 days	All ATO systems, website running intermittently	• Incorrect storage hardware installation.
22 June 2017	3 hours	All ATO systems	• Hardware failure on a server, leading to Active Directory domain controller failure.
5 July 2017	5 hours	All ATO systems	• Applications running incorrectly.
25 September 2017[a]	6 hours	All ATO systems, website running intermittently	• Applications running incorrectly.

Note a: Over the weekend of 23–24 September, the ATO undertook a systems upgrade. This was part of a planned program of regular system maintenance to update and implement upgrades to its systems. In bringing the systems back online on Monday 25 September, the ATO identified issues affecting users of the Tax Agent Portal and made a decision to take some of the online services, including ATO Online and the Tax Agent, BAS and Business Portals, offline in order to rectify the problem immediately.

Source: ANAO analysis.

[11] Australian Taxation Office, *ATO systems report*, June 2017, p. 2. Available from <https://www.ato.gov.au/About-ATO/Access,-accountability-and-reporting/In-detail/ATO-systems-report/> [accessed 14 July 2017].

1.17 The two significant system failures occurred in December 2016 and February 2017, resulting in outages of 10 days and five days respectively.[12] These two system failures were caused by problems with the (then) new storage area network (3PAR storage) solution.[13] The ATO acknowledged a detrimental effect on users but noted no taxpayer data had been lost, and stated that the problems had been rectified for Tax Time 2017. In June 2017, the ATO released a report into the system failures of December 2016 and February 2017. Based on post incident reviews, the *ATO systems report* included 14 recommendations to improve the resilience and availability of systems and services.

1.18 The reaction of external stakeholders to the outages in December and February was primarily negative. A press report summarising the reaction noted:

> ATO's services have been continually taken offline for hours, proving especially frustrating for Australians looking to lodge their returns in the lead-up to tax time, and creating tension between the agency and tax professionals.[14]

1.19 The ATO has recognised the impact of outages:

> We acknowledge the more regular nature of these incidents recently continues to impact on those stakeholders – tax practitioners, the superannuation industry and digital service providers – who rely on the availability of our systems to run their business.[15]

1.20 Public reaction to the outages and the ATO's response indicate a possible gap between external stakeholder expectations and the ATO's service offering. One way to address this issue is through service commitments, which are publicly stated standards for services, and can explicitly or implicitly relate to the availability of services. Ideally, any such commitments should be consistent with tolerances for the availability of services that are specified in contracts with external ICT service providers.

Audit objective and scope

1.21 The objective of the audit was to assess whether the Australian Taxation Office has effectively responded to recent system failures and unscheduled outages.

1.22 To form a conclusion against this objective, the ANAO adopted high-level criteria that the ATO:

- effectively responded to the particular system failures and outages;
- revised its ICT governance, systems and processes in line with the agreed recommendations in the post incident reviews of the system failures; and

[12] The unscheduled outages that occurred between June and September 2017 had much shorter durations, were within or close to the tolerances to restore services for a Priority 1 and 2 system failure, and are not examined in detail in this audit.

[13] 3PAR is a HPE proprietary storage area network device. A storage area network is a dedicated high-speed network (or subnetwork) that interconnects and presents shared pools of storage devices to multiple servers.

[14] Media report in the Canberra Times, available from <http://www.smh.com.au/business/the-economy/our-it-systems-arent-bound-by-commercial-service-standards-says-ato-20170803-gxorv1.html> [accessed 8 August 2017].

[15] ATO's media release, available from <https://www.ato.gov.au/Media-centre/Media-releases/Certainty-for-stakeholders-who-rely-on-ATO-systems/> [accessed 28 August 2017].

- has established and met service commitments and outage tolerances for ICT system availability.

1.23 In undertaking the audit, the ANAO:

- assessed the actions taken by the ATO in response to the system outages, focusing on those in December 2016 and February 2017;
- examined whether effective controls are in place to reduce critical system outages, including the resumption of services with an effective—and tested—business continuity management plan;
- assessed the implementation of the identified 14 key areas for improvements, as reported in the June 2017 *ATO systems report*; and
- reviewed the management relationship with contracted ICT service providers, including service level agreements and performance reporting measures.

1.24 The audit was conducted in accordance with the ANAO Auditing Standards at a cost to the ANAO of approximately $225 200.

1.25 The team members for this audit were, Alex Doyle, Mark Harradine, Judy Jensen, Alison Millea, Steven Favell and Andrew Morris.

2. Responding to system failures

Areas examined

The ANAO assessed the ATO's incident management response to the system failures in December 2016 and February 2017, including as part of its business continuity processes. The ANAO also assessed if the ATO investigated the system failures to inform the ongoing management of its ICT environment.

Conclusion

The ATO's responses to the system failures and unscheduled outages were largely effective, despite inadequacies in business continuity management planning relating to critical infrastructure. The post-incident reviews commissioned and conducted by the ATO have informed the ongoing management of its ICT environment, including through strategies and actions to improve ICT governance, strengthen business continuity processes and address availability and resilience gaps in systems infrastructure.

Area for improvement

The ANAO made a recommendation aimed at improving business continuity processes to address risks to critical infrastructure that may lead to system failures (paragraph 2.10).

Did the ATO invoke effective business continuity processes?

In response to the incidents in December 2016 and February 2017, the ATO invoked its business continuity management plan, but the plan included limited actions to correct ICT system failures associated with critical infrastructure including data centres. The business continuity processes also did not recognise weaknesses in ICT design—particularly that the system recovery tools used to restore ICT services were on the affected storage area networks—which resulted in services not being fully restored for ten days for the December 2016 incident and five days for the February 2017 incident. Despite limited planning for critical infrastructure failure, the ATO's responses to the incidents were largely effective, as it worked closely with the contracted ICT service providers to identify the system fault and restore services in line with activation guidelines, but could have better communicated with stakeholders throughout the incidents.

2.1 The ATO Business Continuity Management (BCM) Plan 'provides a framework for reducing risk, building resilience, identifying contingency arrangements and managing crisis situations'.[16]

2.2 BCM for ICT services in the ATO has two interrelated elements.

- An enterprise-wide BCM framework—focussed on risk management and bringing senior level management attention to bear on incidents, to respond to the situation, restore services and provide a means to coordinate communication.
- IT Service Continuity Management (ITSCM)—a component of BCM focussed on the process for managing ICT-related risks that could seriously affect the business services.

[16] Australian Taxation Office, *ATO Business Continuity Plan*, 2017, p. 3.

ITSCM aims to ensure that the contracted ICT service providers deliver the minimum performance levels of the ICT systems by reducing the risk to an acceptable level and planning for the recovery and restoration of services.[17]

Risk identification and management

2.3 The December 2016 and February 2017 incidents highlight that the ATO did not have a sufficient level of understanding of system failure risks. The ATO's risk management[18] and BCM processes did not include an assessment of risks associated with storage area networks, which were a potential single point of failure. Moreover, BCM processes were limited in planning for critical infrastructure and ICT system failure to the data centres.

2.4 As a consequence, the ATO—including DXC and Leidos—were not prepared for the possibility of complete system failure caused by storage failure. The ATO did not have a secondary enterprise system in place, other than a disaster recovery procedure.[19] At that time, alternate storage solutions through cloud services were considered for performance purposes but not fully implemented.[20]

2.5 Reflecting the non-identification of storage area network risks, the system recovery tools used to restore ICT services—data management, system monitoring and backup/restore—were in the same data centre on the affected storage area network. The system failure meant that these tools were unavailable, and there were no backup or redundant system recovery tools available on other ICT systems to detect and analyse the incident, and to support efforts to recover and restore services.

2.6 As part of its BCM processes, the ATO conducts a business impact analysis to identify business processes that are critical to its continued operation, determine maximum acceptable outages and design treatments to address the risks of outage. The ATO did not identify risks associated with the system recovery tools being on the storage area network as part of its business impact analysis or other BCM processes. The ATO's BCM processes were not sufficiently developed to identify and treat risks of system failure relating to critical infrastructure systems that have a single point of failure.

2.7 The ITSCM administrator, Leidos, also had not identified through the ICT design of the system that the storage area networks were a single point of failure. Issues that could have alerted Leidos to this risk included that the ICT design: specifically excluded an automatic failover; did not include access to system recovery tools; and would not handle multiple network drive failures.

2.8 The ITSCM framework does not prescribe a review of risks for proposed system changes, such as new and replacement system components. This approach relies on the existence of appropriate change management processes, in which specification and approvals from a change

[17] The ITSCM is administered under contract by Leidos as part of its service integration function.

[18] The ATO's risk registers did not include risks associated with storage area networks.

[19] A secondary system or redundant site is a recovery strategy involving the duplication of key ICT components, including data or other key business processes, which allows rapid recovery of services.

[20] Since the December 2016 and February 2017 incidents, the ATO has procured cloud computing services with three contracted ICT service providers (discussed in Chapter 4). The ATO advised that the focus on adopting cloud computing services was to improve performance and availability of the services during Tax Time.

advisory board mitigate risks. The ITSCM framework requires an awareness of change management processes, including whether there had been sufficient assessment of the likelihood and consequences of system failures arising from system changes. In this respect, the ATO did not provide evidence that approved hardware and configuration system changes to the ICT system had been considered (refer following box).

Upgrade of ageing midrange storage system with 3PAR storage area network

In mid-2015, the ATO announced a decision to replace ageing midrange storage with a state-of-the-art solution. The objective was to reduce the risk of system failure by replacing existing storage infrastructure with the [then] new 3PAR storage area network (3PAR SAN) solution from Hewlett Packard Enterprise. According to the ATO, the 3PAR SAN solution would refresh existing storage infrastructure that was end of life and introduce improvements, including faster processing, reduced costs and significant simplification to the storage environment.

The 3PAR SAN refresh changed the ATO's management of midrange data and so altered the risk profile for services utilising this data. Despite an objective that the 3PAR SAN would reduce the risk of system failure, the ATO did not formally consider the risk implications of the new 3PAR SAN, or receive information on risk implications from the SAN provider (DXC) or the contractor (Leidos) responsible for ITSCM.

2.9 Weaknesses in enterprise-wide BCM and ITSCM processes indicate a lack of coordination and integration in the ATO in identifying and treating risks to the operation of critical ICT infrastructure.

Recommendation no.1

2.10 The ATO updates its Business Continuity Management, IT Service Continuity Management and Risk Management frameworks to improve and better integrate the identification and treatment of risks to critical infrastructure that may lead to system failures.

Australian Taxation Office response: *Agreed.*

2.11 *In the 12 months since the ATO System Outage, IT Service Continuity Management has focussed on IT technical architecture and design and operational risk management to strengthen the identification and treatment of risks to critical IT infrastructure that may lead to system failures.*

2.12 *IT Services Continuity Management provides risk information and progress reports for consideration within the broader Business Continuity Management operational framework to the appropriate governance committees.*

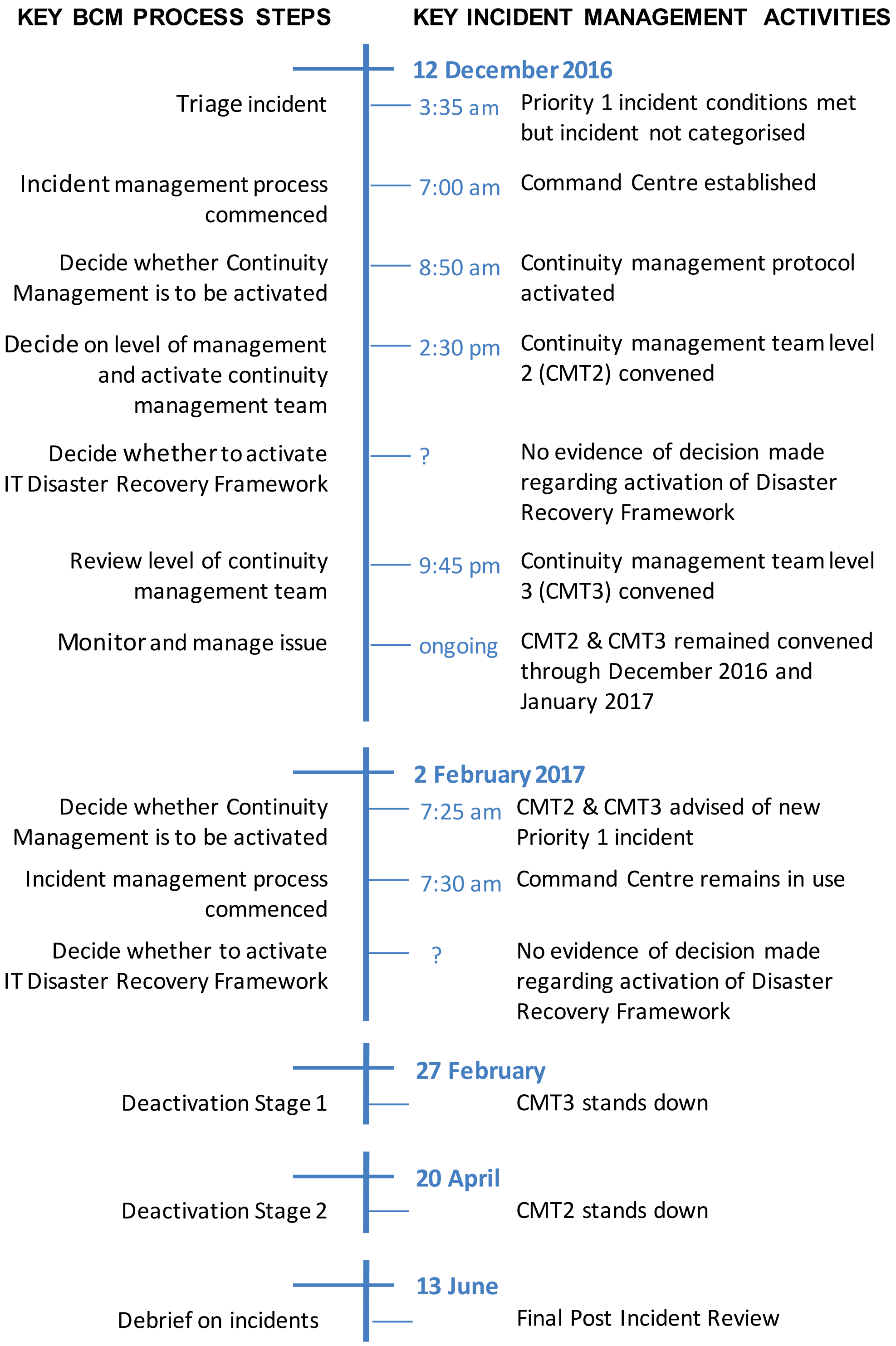
2.13 *Comprehensive frameworks and governance arrangements continue to be strengthened to ensure Business Continuity for ATO, clients and partners.*

Responses to the incidents

2.14 In contrast to risk identification, treatment and business continuity planning, the ATO was better set up to respond to incidents—it had developed BCM activation guidelines and practised for a range of disruptive events, including through annual simulation exercises.

2.15 Figure 2.1 summarises the key steps identified in the BCM activation guidelines against the incident management activities undertaken in the December 2016 and February 2017 incidents. It shows that the ATO managed the incidents in line with the key steps.

Figure 2.1: Steps in the BCM activation guidelines, against the incident management activities in the December 2016 and February 2017 incidents



KEY BCM PROCESS STEPS		KEY INCIDENT MANAGEMENT ACTIVITIES
	12 December 2016	
Triage incident	3:35 am	Priority 1 incident conditions met but incident not categorised
Incident management process commenced	7:00 am	Command Centre established
Decide whether Continuity Management is to be activated	8:50 am	Continuity management protocol activated
Decide on level of management and activate continuity management team	2:30 pm	Continuity management team level 2 (CMT2) convened
Decide whether to activate IT Disaster Recovery Framework	?	No evidence of decision made regarding activation of Disaster Recovery Framework
Review level of continuity management team	9:45 pm	Continuity management team level 3 (CMT3) convened
Monitor and manage issue	ongoing	CMT2 & CMT3 remained convened through December 2016 and January 2017
	2 February 2017	
Decide whether Continuity Management is to be activated	7:25 am	CMT2 & CMT3 advised of new Priority 1 incident
Incident management process commenced	7:30 am	Command Centre remains in use
Decide whether to activate IT Disaster Recovery Framework	?	No evidence of decision made regarding activation of Disaster Recovery Framework
	27 February	
Deactivation Stage 1		CMT3 stands down
	20 April	
Deactivation Stage 2		CMT2 stands down
	13 June	
Debrief on incidents		Final Post Incident Review

Source: ANAO, drawing on ATO Business Continuity Management activation guidelines and Meeting Minutes in the Continuity Management Teams, Level 2 and Level 3.

2.16 Further, the ANAO's examination of the post-incident review activities, including meeting minutes of the ATO's continuity management teams, found that the management of the incidents was largely effective. The ATO worked with the contracted ICT service providers—in particular DXC and Leidos—to identify the system fault and restore services. Upon notification of the incident, the BCM team followed the BCM Triage Framework and identified business impacts, coordinated the initial response efforts, and engaged the Continuity Management Teams. Despite these efforts, services were not fully restored for ten days for the December incident, and another five days for the February incident.[21] The ATO communicated to internal and external stakeholders throughout the incidents, but there was scope to more clearly explain the impact on services rather than systems (as discussed in Chapter 3).

2.17 While the ATO's management of the responses to the system failures were largely effective, it is notable that the ATO did not invoke the ICT disaster recovery framework on either occasion. For example, meeting minutes from the Continuity Management Team, Level 2 (CMT2) for the December 2016 system failure show that immediate restoration to services was impossible, given that the system recovery tools needed to run the restoration protocol were stored on the affected storage area networks. At this point, the conditions for an ICT disaster were met, according to the ATO's ICT disaster recovery framework. However, there was no path to system recovery and restoration of services even if the ICT disaster recovery framework had been invoked, as the ATO had not planned for an incident of system failure to critical infrastructure.

2.18 In this context, the ATO's Continuity Management Teams (CMT2 and CMT3) responded to the incident in the absence of a plan or effective ICT disaster recovery framework—with all available ATO resources, including DXC and Leidos, committed to managing the incident and restoring services.

2.19 The ATO concluded that no taxpayer data was lost as a result of the system failures and revenue was not impacted.[22] To reach these conclusions, the ATO undertook a number of data integrity activities and conducted an internal questionnaire of relevant system owners to determine whether all data had been reconciled following the SAN outages, as outlined in the following box. While these were detailed processes, if the ATO wanted to gain greater assurance it could conduct further targeted checking, including a data reconciliation assessment against backup data.

[21] Critical services were progressively restored from four days after the system failure.

[22] The Commissioner's foreword in the *ATO systems report* states that 'no taxpayer data has been lost or compromised as a result of the outages and government revenue for 2016–17 has not been impacted'. Australian Taxation Office, *ATO systems report*, June 2017, p. iii.

Data assurance activities for the SAN outages

Prior to the December 2016 and February 2017 system failures, the database information on the ATO's ICT systems was replicated to a secondary data store at 15 minute intervals. Throughout the recovery and restoration process, data integrity was a key focus and priority for the ATO, with the aim of ensuring that recovery activities preserved data.

Between February and June 2017, data reconciliation assurance was conducted on affected systems to maintain data integrity. Key activities undertaken were to:

- develop a list of affected services and identified system owners (February 2017);
- develop a data reconciliation evidence signoff questionnaire (March 2017);
- contact system owners to advise of assurance processes, their responsibilities, and the evidence required to support signoff (March 2017);
- distribute a questionnaire to system owners/delegates (March 2017);
- collate and analyse responses to the questionnaire (April 2017 to June 2017); and
- confirm that all responses were endorsed by SES system owners (June 2017).

Data reconciliation questionnaires were issued to the system owners of the 98 systems that were affected by SAN outages. Seventy systems did not require data reconciliation to be conducted as they were not directly impacted. For the other 28 systems, data reconciliation was required.

According to the ATO, the data reconciliation verified that ATO data was either recovered, restored or that no further action was required.

Did the ATO investigate the system failures to inform the ongoing management of systems?

The ATO undertook extensive investigation into the system failures to understand their cause and inform the ongoing management of its broader ICT environment. The ATO commissioned key reviews into the system failures that resulted in eight reports on the cause and response to the failures, ICT governance, and the extent of availability and resilience gaps in the ICT environment. A major outcome of the reviews was the identification of 14 key areas for improvement that fall into five general themes: principles informing the ATO's ICT design; correcting the identified system faults; enhancing ATO capability to support infrastructure design and ICT governance; incident responses for the ATO and the wider tax system; and managing communications and business resumptions with stakeholders.

2.20 Since the December 2016 and February 2017 incidents, the ATO has commissioned reviews[23] and taken account of the findings. Table 2.1 summarises the key reports that detail the cause and response to the incidents, governance arrangements and further resilience risks to the ICT systems. Of note, the ATO released the *ATO systems report* in June 2017, which stated:

> This report provides our current understanding of the causes of this failure, the impacts on our stakeholders, analysis of ATO responses and lessons for improved services in the future. The lessons learned are already being acted upon by the ATO, and they have relevance across the tax and superannuation systems, and for others who use or rely on complex IT systems.[24]

Table 2.1: Key reports that detail the cause and response to the two incidents, governance arrangements and further risks to the ATO's ICT systems

Report title	Date issued	Report theme	Coverage of the report
ATO Storage Situation Briefing	February 2017	▲	DXC report on the preliminary findings and steps taken by DXC to address the system failures. [internal ATO report]
Initial Incident Report - SAN outages	February 2017	▲ ●	A preliminary briefing on the cause of the system failures. [internal ATO report]
Post Incident Review (Draft v9.0)	June 2017	● ■	PricewaterhouseCoopers (PwC) prepares a (final) draft post incident review, after several draft submissions were submitted to the ATO between February and June 2017. [internal ATO report]
Post Incident Review: ATO response to system incidents—December 2016 and February 2017	June 2017	● ■	ATO completes the Post Incident Review, with amendments from the PwC draft post incident review. [public report]
ATO systems report	June 2017	▲ ● ■	A report that explains what happened to the ATO's ICT systems, impacts on stakeholders, ATO responses and what the ATO is doing to improve services. [public report]
HPE Review: Products, Services and Relationship Report	July 2017	●	An internal audit report of the arrangement with Hewlett Packard Enterprises, to identify risks exceeding ATO's risk tolerances associated with delivery, management and oversight arrangements, in the context of the broader ATO environment. [internal ATO report]

[23] Technical advice was sought from DXC Technology, PricewaterhouseCoopers (PwC) and the ATO's Chief Technology Officer Group.

[24] Australian Taxation Office, *ATO systems report*, June 2017, p. iv.

Report title	Date issued	Report theme	Coverage of the report
Deed of Resolution between the ATO and DXC Technology	July 2017	▲	An agreement between the ATO and DXC Technology for outstanding work activities by DXC, including a financial settlement for the pre- and post-incident activities. [internal ATO report, restricted to ATO Executives].
Infrastructure Resilience and Availability Review	September 2017	🟦	PwC conducted a broad investigation into the ATO's ICT infrastructure deployment, including cloud computing, and assessed key resilience gaps. [internal ATO report].

KEY:

Cause and response to system failures	▲
Governance review	🟢
Post incident reviews and resilience risk	🟦

Source: ANAO analysis.

Cause and response to system failures

2.21 In late February 2017, DXC provided the ATO with a situation brief on the December 2016 and February 2017 system failures.[25] The brief described, in technical terms, the key events that caused the outages. The preliminary technical assessment of the system outages, as reported by DXC, is summarised in Appendix 2.

2.22 At the time of that brief, DXC indicated it would migrate all data off the failed storage array and return the storage array for a comprehensive factory failure analysis.[26] The 'failed' SAN device was replaced with 'new' storage devices at both the Sydney Data Centre and the Western Sydney Data Centre.[27]

2.23 The ATO's Initial Incident Report (February 2017) also provided a preliminary view on the causes and impacts of the outages in December 2016 and February 2017, and a summary of the incident recovery process. The report indicated that the outages were caused by hardware failures within DXC's SAN servers used to store the majority of the ATO's midrange data and applications—and not the data storage virtualization technology[28] (RAID) as reported in the

[25] *ATO Storage Situation Briefing*, DXC Technology, February 2017.

[26] DXC decommissioned the failed 3PAR SAN supporting the production environment by July 2017. The ATO is expecting DXC to provide the results of a forensic analysis of the failed 3PAR SAN early in 2018.

[27] For the new production environment the new storage devices were—one XP7 SAN at the Sydney Data Centre and one XP7 SAN at the Western Sydney Data Centre. For the new development and test environment the new storage devices were—one 3PAR SAN at the Sydney Data Centre in combination with the original 3PAR SAN at the Western Sydney Data Centre. This new configuration represents a major upgrade in infrastructure, providing for cross-site data asynchronous replication of the production environment.

[28] According to ISACA—the professional association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems—a Redundant Array of Inexpensive Disks (RAID) provides performance improvements and fault-tolerant capabilities via hardware or software solutions, by writing to a series of multiple disks to improve performance and/or save large files simultaneously.

situational brief. The failures in the SAN servers caused the ATO's internal systems to fail, including Siebel and Sharepoint, and system failure of external client-facing systems.

2.24 The Initial Incident Report noted that DXC restored the main storage server early in the response to the outage rather than transitioning to a different storage server. According to DXC, despite the main storage server suffering from stability issues, its ongoing use would result in services being restored more quickly.[29]

2.25 In respect of impacts to stakeholders, the report rated the effect on external clients as 'significant'.

> Individuals could not lodge or complete payments, tax agents were unable to access Tax Agent Portal and business clients were unable to do business with the ATO's systems.[30]

2.26 The report noted a 'mixed reaction' from clients and suggested a survey of clients would assist in determining how to manage communications in the event of future incidents. It also noted that the impact on staff was 'considerable' and that the unavailability of internal systems 'meant that transactional work could not be completed as well as normal business as usual work'.[31]

2.27 Since the release of the situation brief in February 2017, the ATO and DXC have jointly investigated the system failures further and have implemented a response that is set out in a Deed of Resolution between the parties.[32] Signed 28 July 2017, the deed established a commercial arrangement pursuant to which the ATO settled with DXC regarding the SAN incidents, and future management of the ICT systems, without DXC being held liable for the incidents. The Commissioner of Taxation advised the Senate Economics Legislation Committee on 30 May 2017 that 'the settlement recoups the key costs incurred by the ATO and provides us with additional and higher-grade ICT equipment'. The ANAO notes that the settlement did provide the ATO with higher-grade SAN equipment. The ATO calculated key costs resulting from the outages, and on the basis of independent legal advice put these costs forward in negotiating further settlement amounts in cash and service credits.

Governance review

2.28 The ATO commissioned PricewaterhouseCoopers (PwC) to provide detailed advice on the system failure in December 2016 (but not February 2017), including technical advice and issues relating to governance.[33] The Draft Post Incident Review prepared by PwC highlighted the requirement for specific actions to be undertaken by the ATO, including:

- Re-architecture of the ICT system for resilience; and

[29] Australian Taxation Office, *Initial Incident Report—SAN outages*, ATO, 2017, p. 6.

[30] ibid., p. 5.

[31] ibid., p. 5.

[32] The Commissioner of Taxation was in communication with the Chief Executive Officer and senior executives of DXC Technology during settlement negotiations. A deed of resolution was prepared, in the understanding that the agreement remained commercial-in-confidence.

[33] The agreed terms of reference were to 'conduct an end-to end review into what happened and why, and what needs to happen to ensure the ATO and the community are not exposed to this type of incident in future'. *Terms of Reference*, released by the ATO on 13 December 2016.

- Strengthening governance, risk and response capabilities.

2.29 The PwC report also outlined a series of recommended improvements for consideration by the ATO. These improvements were mostly agreed to by the ATO and were included in the June 2017 *ATO systems report*, discussed in more detail in the following paragraphs.

2.30 The final Post Incident Review was prepared and released by the ATO. The report draws on PwC's Draft Post Incident Review, and focuses on the operation of the enterprise-wide BCM framework. The report also describes the impacts and experiences of different stakeholders, including tax professionals, superannuation industry members, software developers and ATO business areas.[34] The review excluded consideration of information technology aspects of the incidents, noting that these were being addressed through the *Infrastructure Resilience and Availability* review and the forthcoming DXC root cause review. The report aligns with material in the *ATO systems report*.

2.31 The *ATO systems report* outlines the causes of the system failures and the impacts on stakeholders, analyses the ATO responses and provides lessons for improved services in the future. The report identifies 14 key areas for improvement that fall into five general themes:

- principles informing the ATO's ICT design;
- correcting the identified system faults;
- enhancing ATO capability to support infrastructure design and ICT governance;
- incident responses for the ATO and the wider tax system; and
- managing communications and business resumptions with stakeholders.[35]

2.32 To complement other investigations underway on the systems failures, the ATO conducted an internal audit into the contract and relationship with DXC, and whether any aspects of the arrangements exceeded ATO's risk tolerances.[36] The internal audit found that while there were no immediate issues apparent in contractual arrangements, there were broader issues surrounding the extent of strategic alignment of the contracted ICT service providers' offerings with ATO business objectives. The report made several recommendations in this regard, and noted that:

> Importantly, at an entity-level, greater definition is required as to how the ATO engages with key vendors, supported by greater analysis and monitoring of arrangements, including periodic reporting to the ATO Executive. In this way, the ATO will better define and achieve strategic value from vendors, with better visibility and control of the breadth of, and reliance upon, vendor arrangements.[37]

[34] Australian Taxation Office, *Post Incident Review: ATO response to system incidents—December 2016 and February 2017*, 2017, p. 3.

[35] The status of the ATO's implementation of the recommended areas for improvement is discussed in Chapter 3 of this audit report.

[36] The ATO's Chief Internal Auditor and Chief Risk Officer undertook a review of arrangements with DXC, to identify any risks exceeding the ATO's tolerance associated with delivery, management and oversight arrangements. According to the ATO's Risk Tolerance Guide, risk tolerance is the level of risk-taking that is acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance relates directly to individual risks and the risk category to which it is mapped. The ATO expresses risk tolerance in terms of a maximum acceptable risk level that combines a likelihood and consequence rating.

[37] Australian Taxation Office, *HPE Review Product, Services and Relationships Report*, July 2017, p. ii.

Post incident reviews and resilience risk

2.33 In response to the findings in the PwC Draft Post Incident Review, the ATO engaged PwC under a separate work order in April 2017 to more broadly investigate the resilience of the ATO's ICT infrastructure. The review was to:

- determine key areas of resilience risk and system availability; and
- identify programs of work to mitigate identified risks and improve the resilience of the ATO's ICT infrastructure.

2.34 The concern addressed was that the pre-incident conditions that contributed to lower resilience characteristics of the SAN—including design, build and operate issues—potentially existed in other areas of the ATO's ICT infrastructure, and that a seemingly minor issue could again result in a disproportionately significant disruption to ATO services. The review was undertaken against PwC's industry framework of resilience in the context of the ATO's vision to operate as a contemporary digital business with world class infrastructure and a core focus on resilience, enabling real-time, direct submission of transactional data by taxpayers and other clients and partners.[38]

2.35 PwC focused on the 'Top 8' applications[39] to examine the resilience and availability risk. PwC found that, 'enough analysis has been done to suggest that the ATO's Top-8 applications are at resilience risk and that any further infrastructure failures will most likely result in material outage and lost business time'.[40]

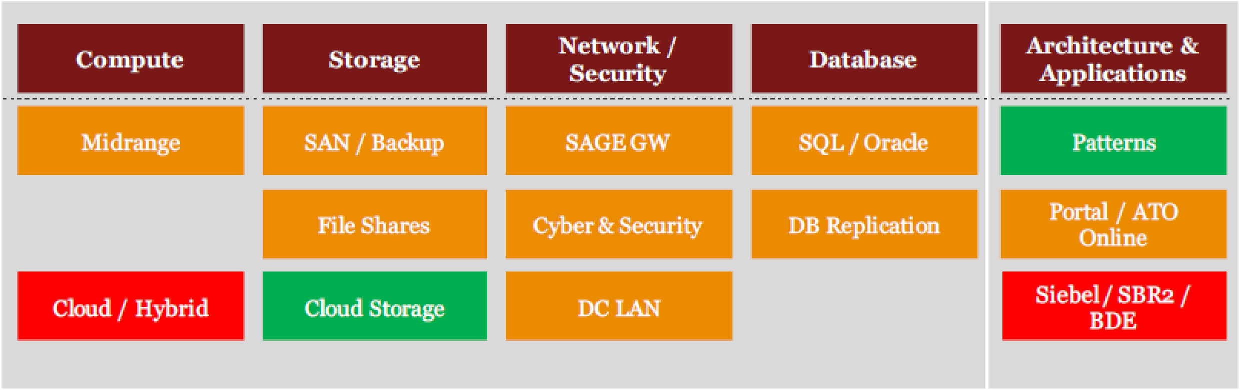
2.36 Figure 2.2 illustrates the summary assessment of risks to resilience in the ATO's ICT system as reported by PwC in the *Infrastructure Resilience and Availability Review*.

[38] PwC, *Infrastructure Resilience and Availability Review,* pp. 6–7, and advice provided by the ATO in January 2018.

[39] The Top 8 infrastructure applications are: SBR 1 and SBR 2, ATO Online, ATO Portal, ABR, ato.gov.au, case management (Siebel) and ICP UI.

[40] PwC, *Infrastructure Resilience and Availability Review*, September 2017, p. 18.

Figure 2.2: Summary assessment of risks to resilience in ATO's ICT system



Compute	Storage	Network / Security	Database	Architecture & Applications
🟧 Midrange	🟧 SAN / Backup	🟧 SAGE GW	🟧 SQL / Oracle	🟩 Patterns
	🟧 File Shares	🟧 Cyber & Security	🟧 DB Replication	🟧 Portal / ATO Online
🟥 Cloud / Hybrid	🟩 Cloud Storage	🟧 DC LAN		🟥 Siebel / SBR2 / BDE

KEY:

🟥 Critical

- Failures of this element ***will*** impact Top 8 applications.

🟧 Warning

- Failures of this element ***will likely*** impact Top 8 applications.
- Basic building blocks are available but some work is required to reduce risk.

🟩 Clear

- The resilience and availability of the underlying infrastructure elements will allow the Top 8 applications to deliver services in the event of a system failure.

Source: ANAO reproduction of data presented in the PwC *Infrastructure Resilience and Availability Review* (September 2017).

2.37 According to PwC, key resilience gaps were identified despite modernisation investments made to legacy technology. These resilience gaps included:

- end-to-end transactions are supported by a combination of 'old' and 'new' infrastructure, including cloud and non-cloud solutions;
- automation of systems is low, with the potential for errors in change and configuration that could impede assurance and accurate data recovery efforts;
- integrated technical monitoring and pro-active risk identification, whereby the identification of resilience risks is hampered by the challenge of extracting data from systems maintained by contracted ICT service providers;
- a gap in the ATO's technical governance—as the service integrator—in the effective management of its ICT environment, the impact of which will be exacerbated by the adoption of cloud services provided by contracted ICT service providers; and
- automated fail-over across system components is not completed for some critical infrastructure systems.

2.38 The ATO has responded to the system failures by addressing the 14 key areas for improvement in the *ATO system report,* which include recommended actions to improve the resilience of the ATO's ICT environment and availability of its systems and services.

3. Initiatives to reduce system failures

Areas examined

The ANAO examined whether the ATO had revised its ICT governance, systems and processes in line with the agreed recommendations in the *ATO systems report*.

Conclusion

The ATO has structured its response to the system failures of December 2016 and February 2017 around the 14 recommendations included in the *ATO systems report*. The ANAO considers that, at November 2017, the ATO had implemented four recommendations and partly implemented the remaining 10 recommendations. The implemented recommendations mainly relate to technical solutions to the particular system failures, while the broader initiatives to strengthen ICT governance and processes are underway. Considerable work is required to implement the recommendations before many of the intended and agreed outcomes are achieved.

Areas for improvement

In implementing the remaining recommendations from the *ATO systems report*, three key matters warrant further attention:

- improving the business continuity framework, including better planning for risks to critical infrastructure and updates with communications processes;
- fully embedding enhancements to system design to reduce resilience gaps; and
- setting timeframes to deliver key initiatives, such as active monitoring systems and the application of general waivers and discretions.

Introduction

3.1 As discussed in the previous chapter, the ATO released the *ATO systems report* in July 2017. Elements of the report outline the ATO's understanding of the impacts arising from the system failures in December 2016 and February 2017, and opportunities for improvement.

3.2 The Commissioner's foreword in the report states:

> Our priority has been, and is, to ensure stability, reliability and availability of our services to the community, our key stakeholders and government. To this end, we have begun implementing a range of measures to enhance the stability and resilience of our systems, which includes the replacement of the faulty hardware that caused the outages.[41]

The report also contains the ATO's recommended improvements—the 14 key areas that fall into five general themes, as shown in Table 3.1.

[41] Australian Taxation Office, *ATO systems report*, June 2017, p. iii.

Table 3.1: Recommended improvements in response to the system failures

Themes and recommendations
Theme 1: Principles informing the ATO’s ICT design
Recommendation 1.1: The design and implementation of our infrastructure requires us to continue to identify the optimal balance of performance, stability, resilience and cost as an overarching consideration. In turn this should shape and inform our future IT sourcing program.
Recommendation 1.2: The ATO’s IT strategy continues to prioritise government reforms, aligns with corporate objectives and has an ongoing focus for a successful implementation of Tax Time 2017.
Theme 2: Correcting the identified system faults
Recommendation 2.1: Replace the current 3PAR SAN at Sydney with new storage infrastructure, the design of which should rebalance performance, stability, resilience and cost factors.
Recommendation 2.2: The ATO should address disk drive errors relating to the 3PAR SAN to minimise the possibility of reoccurrence of the incidents experienced. This should include replacing the affected drives and / or ensuring that updates to firmware used in operating the drives have been developed, implemented and fully tested.
Recommendation 2.3: Ensure that the ATO’s data management, monitoring and recovery systems are housed in a separate, independent, storage area to remove the dependency of these control systems on the principal SAN. We should also re-architect these control systems to provide ‘always on’ capability.
Recommendation 2.4: Review and risk assess ATO infrastructure to improve resilience and mitigate the impact of a complete data storage failure whilst continuing to rebalance performance, stability, resilience and cost factors. This should include: • increasing and improving fail-over features at both the database and application levels to ensure appropriate back-up • enabling applications to interact with standard SAN monitoring and resilience features.
Theme 3: Enhancing ATO capability to support infrastructure design and ICT governance
Recommendation 3.1: Enhance the ATO’s IT capability pertaining to infrastructure design and implementation planning (particularly relating to resilience and availability). This should be done having regard to recruitment, engagement of contractors, and whole-of-government strategies.
Recommendation 3.2: Improve the design and governance capability and governance processes with specific attention given to: • understanding resilience objectives and risk appetite within the context of desired performance, stability and cost constraints • implementing governance processes and improving ATO design capability to better ensure the build of IT systems by contractors is compliant with approved designs.
Recommendation 3.3: Improve the analytics function of the ATO’s centralised logging capability while still applying the appropriate balance of performance, stability, resilience and cost factors, with a particular focus on: • early detection, fault finding and proactive problem management • resolution approaches, including active monitoring, analysing issue trends and response evaluation.
Theme 4: Incident responses for the ATO and the wider tax system
Recommendation 4.1: Enhance the ATO’s existing IT-related business continuity management functions to provide an enterprise-wide focus on preparing for, testing, and responding to disruptive events. This should include establishing a permanent and dedicated resilience ‘run’ function again within the appropriate balance of performance, stability, resilience and cost factors.

Themes and recommendations
Recommendation 4.2: Consolidate, streamline, update, and simplify existing business continuity management documentation to clearly articulate the relationship between and accountability for business continuity, disaster recovery, and resilience planning.
Recommendation 4.3: The ATO should assist key stakeholders understand our business continuity strategies to assist them in improving their own continuity strategies. This will help improve the resilience of the entire tax and super system. These strategies should be designed with a whole of system approach to ensure they are streamlined and easily integrated.
Theme 5: Managing communication and business resumption with stakeholders
Recommendation 5.1: In the event of an unscheduled, high impact, disruption to ATO services, to support the transparency and regularity of our communications, we need to improve key stakeholder communications, ensuring they are tailored to each particular stakeholder's experience.
Recommendation 5.2: Where ATO systems outages impact on a stakeholder's business model or their forward planning, the ATO takes these factors into account in setting clear expectations for how waivers / discretions will be exercised in these circumstances, within the boundaries of the law.

Source: *ATO systems report*, June 2017.

3.3 The ATO has monitored the implementation of the 14 recommendations and in September 2017 provided the ANAO with a document that outlined its implementation approaches and included an assessment of implementation status. At that time, the ATO considered that two recommendations[42] had been implemented and the other 12 were on track for implementation. Of the 12 recommendations being implemented, four had target completion dates and the other eight were in planning or were ongoing without a target completion date. The ANAO considers that, as at November 2017, four recommendations[43] had been implemented. While strategies and activities were underway to implement the other 10 recommendations, for those recommendations without a completion date or milestones it is not possible to assess whether implementation is on track.

Has the ATO reviewed and updated its ICT design, including for alignment with corporate objectives?

The ATO has examined its ICT infrastructure to identify availability and resilience gaps, and has reviewed and updated its IT Program of Work and associated projects to focus on improving availability and resilience, particularly for the more important applications. The reviews have identified that further work is required to improve system design and deliver corporate objectives. At the time of audit fieldwork, there were no target dates or milestones for completing this work or implementing the two recommendations in this theme.

[42] Recommendation 2.1—replace the current 3PAR SAN; and Recommendation 2.2—address disk drive errors relating to the 3PAR SAN.

[43] In addition to Recommendations 2.1 and 2.2, the two additional recommendations are: Recommendation 2.3—data management, monitoring and recovery systems are housed in a separate, independent, storage area; and Recommendation 5.1—support the transparency and regularity of communications to stakeholders.

Improving ICT system design

3.4 Recommendation 1.1 requires the ATO to identify the optimal balance of performance, stability, resilience and cost as an overarching consideration in its ICT design. Activities to respond to this recommendation have included a review of the ATO's IT Program of Work and aspects of an IT Systems Improvement Program.

3.5 The ATO reviewed its IT Program of Work in February 2017 to strengthen systems and improve systems resilience, as that underpins the digital delivery of services. The strategy has placed increased emphasis on strengthening delivery platforms that underpin digital services, and includes a commitment to:

- support intermediaries that provide taxation services—by increasing the availability of systems and reducing scheduled outages; and
- an agile enterprise system that can support rapid and continuous change—by ensuring the systems remain stable and secure.

3.6 An IT Systems Improvement Program has been designed with a focus on improving the availability and resilience of the Top 8 applications to a 'gold standard'[44], including investment in cloud computing services. Currently in the first year of a four-year program, activities in the program incorporate elements to address the resilience gaps outlined in the Infrastructure Resilience and Availability Review.[45]

3.7 In July 2017, the ATO issued the set of ATO Enterprise Architecture Principles—a guidance document to inform architecture work on performance, reliability, availability, flexibility and cost. A comment in the principles is the ATO's commitment that 'users and partners shall be the focus in all solution design: client-centricity to business services is a key objective and outcome that is relevant to all aspects of the architecture, from business processes through to technical solution'.[46] The principles address reliability and availability through discussion of resilience, although the intended tolerances for availability, reliability and resilience are not quantified.[47]

3.8 The ATO has undertaken a transformation program in recent years to improve users' experience through the introduction of multiple digital services channels. According to the ATO, this initiative has resulted in an increase in transactional volumes by users. Going forward, the

[44] ATO advice of 7 September 2017 in document *Improving ATO Systems, for Availability, Stability and Resilience*.

[45] *Infrastructure Resilience and Availability Review*, PwC, September 2017. In deciding the scope of the work, the ATO and PwC agreed not to review all infrastructure components. Instead, priority was given to the 'Top 8' applications from a broad infrastructure perspective. The review conducted an end-to-end analysis of the systems supporting the applications, and conducted an interactive scenario analysis—a process of analyzing possible future events by considering alternative possible outcomes.

[46] Australian Taxation Office, *ATO Architecture Principles – Fundamental guidance for all ATO architecture work*, July 2017 [internal report]. As defined in the principles, 'Architecture principles should drive organisational transformation, and thus should be a blend of pragmatic and aspirational statements. They should be used to inform and guide architectural decisions, should serve as assurance benchmarks, and should align with ATO's strategic directions'.

[47] The principles state that 'all solutions shall be designed and built with a balance of certain qualities in order to achieve an effective, efficient, and runnable solution. Qualities that are to be considered include (at a minimum): performance, reliability, flexibility, agility, security, availability, operability, maintainability, usability, scalability, and cost'. Further, the principles only provide qualitative target statements—such as to be effective and efficient—rather than measurable performance targets.

program will need to include initiatives to deliver on the ATO Architecture Principle and meet the growing expectations of users and business partners in respect of reliability and availability.

Prioritising the IT Program of Work to meet government and corporate objectives

3.9 The ATO advised that it is committed to supporting the government's ICT agenda, and is examining how best to align corporate objectives with the prioritisation of ICT investment strategies. An initial step has been to revise the IT Program of Work to explicitly prioritise government reforms and align with corporate objectives. Further, the *ATO Corporate Plan 2017–18* reports that the ICT strategy will help the ATO to meet its strategic objective of providing clients with reliable services by enabling streamlined and seamless services.[48]

3.10 The ATO has a priority focus on achieving a successful Tax Time[49] each year. In this regard, the Commissioner's foreword in the *Annual Report 2016–17* stated:

> We were very conscious of the need to restore confidence in our services, performance and integrity. Consequently, we adjusted our priorities and efforts, instigated a number of reviews, responded to external scrutineers, and drove an intensive program to remedy and develop our ICT systems ready for Tax Time 2017 and beyond.
>
> … while we have had some intermittent issues with system performance, availability for Tax Time 2017 is at the same level, if not better than in previous years.
>
> … we moved our website ato.gov.au to be hosted in the cloud, providing a more stable environment for peak period system demands and flexibility to release content to the community 24/7.[50]

3.11 As at October 2017, the ATO had processed a large number of lodgements in Tax Time 2017, with:

- 7.7 million lodgements from self-preparers and tax agents, up on 2016;
- 6.2 million refunds issued, totalling more than $17.4 billion; and a
- 30 per cent reduction in complaints compared to the same time last year.[51]

3.12 The initiatives undertaken by the ATO in replacing the 'failed' 3PAR storage area devices in the lead up to Tax Time mitigated the risk of a similar critical infrastructure system failure caused by storage arrays. Nonetheless, further initiatives are required to ensure the ongoing availability, reliability and stability of the infrastructure from future system failures to critical infrastructure.

3.13 At the time of audit fieldwork, the ATO did not have a target completion date, or milestones, for implementing either of the recommendations in Theme 1, relating to reviewing and updating the ICT design.

[48] Australian Taxation Office, *ATO Corporate plan 2017–18*, p. 13. Available from: <https://www.ato.gov.au/About-ATO/About-us/In-detail/Strategic-direction/ATO-Corporate-plan-2017-18/> [accessed 10 October 2017]

[49] Tax Time refers to the time of the year where the ATO most intensively processes income tax returns, and is usually from early July to the end of October.

[50] Australian Taxation Office, *Commissioner of Taxation Annual Report 2016–17*, ATO, 2017, pp. ii to iii.

[51] ibid., p. ii.

Has the ATO implemented a new storage strategy?

A new storage strategy was approved, and the failed storage area networks were replaced and independently certified for use in readiness for Tax Time 2017. Control systems used to manage data, monitor systems and restore services are now hosted on separate infrastructure. The implementation of the new IT Systems Improvement Program has improved resilience to system failures for most services, although further planned initiatives remain a work in progress. This recommendation is being implemented, and the other three recommendations in this theme have been implemented.

Replacing faulty storage drives

3.14 In February 2017, the ATO approved the new storage strategy proposed by DXC. The strategy proposed to migrate all data off the failed storage array, and replace the storage network devices with new XP7 storage components at both the Sydney Data Centre and the Western Sydney Data Centre. The design was assessed by the ATO's Architecture Group and independently assured.[52] Final approval to proceed with the strategy was provided by the ATO IT Design Direction Committee.

3.15 The work to replace the 'old' 3PAR SAN was carried out in the Rebuild Program under the SAN Migration project (see box below), and included replacing the damaged disk drives, replacing all optical cables, updating the firmware and independent testing.

3.16 DXC decommissioned the failed 3PAR SAN supporting the production environment by July 2017. The SAN migration was completed as a phased approach once the new XP7 SAN was installed. A final report and certification was issued in June 2017.

3.17 The defective 3PAR SAN was sent to HPE laboratories in the USA for forensic analysis into the root cause of the failed storage drives. A report from DXC is expected in early 2018.

Summary of the SAN Migration Storage Design

The scope the SAN Migration project was to 'stand up' dual XP7 SANs in the Sydney and the Western Sydney Data Centres. The storage environment includes replicated storage arrays across data centres, a feature absent from the 'original' 3PAR SAN-supported environment. The updated storage configuration will be monitored for capacity and performance.

According to DXC, the dual XP7 storage configuration provides better performance. In the event a storage drive may be failing, it will not lock the troubled drive but use one of the spare storage drives to rebuild itself. The storage array will continue to write to the disk until it is completely rebuilt on the spare drive and then lock out the failing drive. This storage configuration provides the ATO with the capability to run its ICT systems even if two storage disks fail simultaneously.

[52] The ATO engaged the services of the CTO Group—a consultancy firm—in response to the system failures of December 2016 and February 2017. The scope of the work was to: assess the ATO's Enterprise Architecture; and provide assurance of the SAN implementation process, specifically targeted at ensuring readiness for Tax Time 2017.

3.18 As discussed in Chapter 2, the ATO commissioned PwC to conduct an *Infrastructure Resilience and Availability Review,* which has supported the ATO to more broadly improve the resilience of its ICT infrastructure.

Redundant systems and improved resilience

3.19 As discussed in paragraph 3.6, the ATO is in the first year of a four-year IT Systems Improvement Program to address the resilience gaps in line with the findings of the *Infrastructure Resilience and Availability Review* (see Figure 2.2 and paragraphs 2.33 to 2.37). The review gave assurance that the key ATO services, including the Top 8 applications, are more resilient to systems failures and provide faster return to operational capability with the implementation of the new storage strategy. The review also noted that further work is required to reduce the risk of broad system failures in the event of a failure of underlying infrastructure elements (see box below).[53]

Status of ATO services, as at November 2017

The *Infrastructure Resilience and Availability Review* examined the ATO's infrastructure for availability and resilience gaps since the implementation of the new ICT storage strategy. The review identified ATO services were:

(a) **more resilient to systems failures and provide faster return to operational capability**—for systems supporting Tax Agent Portal, Business Portal, BAS Agent Portal, ATO Online (which includes MyTax and Individual Services), ATO.gov.au and the underlying enabling applications; and

(b) **available across both data centres**—such as Australian Business Register (ABR), e-commerce Platform (SBR1) and Siebel (ATO's case management system).

Work is underway to re-architect other key applications, such as SBR2, to further improve availability and resilience, and enable applications to the cloud platform.

Has the ATO enhanced its systems capability and monitoring?

The ATO has implemented several initiatives to enhance systems capability and resilience, including accelerating the use of cloud computing services and in-house oversight on infrastructure architecture. Activities are underway to implement active monitoring systems and centralised logging of transactional events across the infrastructure—this recommendation is being implemented, as are the other two recommendations from this theme.

Enhancing systems capability

3.20 In early 2016, the ATO commenced a review of its IT Program of Work, including service arrangements with contracted ICT service providers, to consider the option of incorporating a hybrid-ICT systems solution for cloud computing services. According to the ATO, engaging in new technology such as the cloud environment would enhance performance and resilience, and be cost effective.

[53] PwC, *Infrastructure Resilience and Availability Review*, September 2017.

3.21 Contract negotiations had started with a cloud service provider. The first of three contracts was signed on 16 May 2016; the second contract was signed on 13 December 2016—the day after the December incident.

3.22 In response to the system failures, the ATO undertook several initiatives to enhance systems capability, including:

- accelerating the implementation of cloud computing services. As at November 2017, the ATO has migrated three of its Top 8 applications to the cloud environment, such as ato.gov.au[54];
- establishing a new branch with oversight of the architecture and ICT design of ATO's enterprise infrastructure, including the ICT systems supported by contracted ICT service providers; and
- engaging external industry expertise for advice on effectively implementing hybrid ICT infrastructure platforms consistent with the ATO's ICT design.

3.23 The *Infrastructure Resilience and Availability Review* also raised concerns about systems assets and applications deployed on the public cloud. Of notable concern was the low level of standardisation across the cloud and hybrid environment, and inadequate technical governance. The ATO advised the ANAO that a review was initiated to examine standardisation and governance arrangements, including technical and service delivery arrangements. The findings of the review were not completed in time for this audit report.

Monitoring systems

3.24 The ATO's investigation into the cause of the system failures in December 2016 identified a shortfall in the monitoring of storage area networks, including the reporting of alerts. As discussed previously, the control, management and monitoring systems relied on the ICT systems that were supporting the impacted services. This aspect of the ICT design extended the recovery process for some applications and services. The new ICT strategy addresses this issue.

3.25 The ATO has initiated steps to improve active monitoring and problem management with the enhancement of operations for the Enterprise Operations Centre, and the Cyber Security Operations Centre. According to the ATO, the Enterprise Operations Centre provides around the clock monitoring of systems operations, including a coordinating capability to facilitate incidents and communications. The Centre provides early detection and reporting of incidents, particularly in the monitoring of services for Tax Time, and releases standardised text messages as a channel of communication in the event of unscheduled outages. The Cyber Security Operations Centre monitors systems for security threats and conducts investigations.

3.26 To further enhance the active monitoring of systems, the ATO is implementing a Security Incident and Event Management capability. In its maturity, the Security Incident and Event Management capability is to receive event data from multiple systems and enable centralised logging of transactional events across the infrastructure.

3.27 The ATO also maintains the Enterprise Service Management Centre, managed by Leidos as a contracted ICT service provider. The Enterprise Service Management Centre contract includes

[54] Contractual arrangements with the three cloud computing service providers are discussed in Chapter 4.

the provision of a service desk for help inquiries, and the delivery of incident and problem management. The ESMC–ATO Service Management framework outlines the responsibilities of the Enterprise Service Management Centre to:

- monitor system performance across the infrastructure;
- provide integrated status view, including systems managed by other contracted ICT service providers;
- coordinate and drive resolution;
- lead and manage priority incidents (Priority 1 and Priority 2); and
- deliver and be responsible for integrated Problem Management.

3.28 As reported in the ATO systems report:

> Analysis of SAN log data for the six months preceding the incident indicated potential issues with the Sydney SAN similar to those experienced during the December outage. While DXC had taken some actions in response to these indicators – including the replacement of specific cables – alerts continued to be reported, indicating these actions did not resolve the potential SAN stability risk. (page iv)
>
> … [the ATO] were not made fully aware of the significance of the continuing trend of alerts, nor the broader systems impacts that would result from the failure of the 3PAR SAN. (page 2)

3.29 Accordingly, Leidos was aware of continuing unresolved issues with the storage area network arrays but did not report these issues to ATO executives. As discussed in paragraph 2.7 to 2.9, Leidos also had a role as the IT Service Continuity Management, and could have identified through the ICT design of the system that the storage area networks were a single point of failure.

3.30 The ATO advised that the performance of Leidos under the obligations of their contract was considered and independent legal opinion sought. The advice was that there was a lack of evidence that a performance breach had occurred. The ATO further advised that it has taken steps to better analyse log data to identify potential infrastructure failures. Given the steps to improve active monitoring and problem management, it would be timely for the ATO to reconsider the roles of the Enterprise Service Management Centre in light of the previous non-reporting of trends and enhanced monitoring through the Enterprise Operations Centre.

Has the ATO improved its incident response processes?

The ATO has reviewed its business continuity framework and identified areas for improvement, with updates to key BCM artefacts including the BCM Team Plan and a *Practical guide to Business Continuity in the ATO*. Further activities are underway to mature the ICT incident management, communication and escalation workflow to better reflect effective planning and response to ICT-related incidents. Forums have been held with superannuation and tax agents to assist them in improving their own business continuity strategies to help improve the resilience of the entire tax and superannuation system. All three recommendations in this theme are being implemented.

Enhancing business continuity planning

3.31 In response to ANAO Audit Report No.16 2008–09 *The Australian Taxation Office's Administration of Business Continuity Management*, the ATO embarked on a program to overhaul its recovery and incident management processes and incorporate a program of continuous improvement. The ATO continues to enhance its BCM functions and governance arrangements to support enterprise-wide services.

3.32 BCM was governed by the BCM Steering Committee until January 2017. The Security and Business Continuity Committee now oversees BCM governance, supported by a senior executive BCM sponsor and a BCM sub-committee. The sub-committee meets on a quarterly basis and reports directly to the Security and Business Continuity Committee. The BCM sub-committee's charter has been drafted and was ratified in October 2017. The first sub-committee meeting was held in mid-October 2017.

3.33 As discussed in Chapter 2, the ATO BCM Plan governs and coordinates the ATO's actions during a business disruption. It provides a framework for reducing risk, building resilience, identifying contingencies arrangements and managing crisis situations. The BCM plan is supported by the ATO's *Chief Executive Instruction for Business Continuity Management and Emergency Planning and Response*, and the BCM activation guidelines.

3.34 In response to the incidents in December 2016 and February 2017, the BCM framework was reviewed with updates completed, or close to being completed, on key BCM artefacts:

- The BCM overview video—that aims to provide guidance for senior executive officers on their BCM responsibilities in the planning, management and response to incidents.
- The *Practical guide to Business Continuity in the ATO*—used to induct new staff with business continuity responsibilities and provide a concise view of the ATO's business continuity management processes. The ATO advised the ANAO that it has also circulated the guide to the ATO Executive, National Program Managers, the Tax Time Steering Committee, the Tax Time Senior Reference Group, and site leaders.
- The BCM Team Plan 2016–17—reflects the organisational approach to business continuity and acknowledges the increased integration with whole-of-government and industry stakeholders.
- The ICT incident management, communication and escalation workflow. Further activities are underway to mature the workflow to better reflect effective planning and response to ICT-related incidents, including risks to critical infrastructure and system failures to the data centres.

3.35 As discussed in paragraph 2.14, the ATO had developed BCM activation guidelines and practised for a range of disruptive events, including through annual simulation exercises, despite shortcomings in risk identification, treatment and business continuity planning. Given the limited planning for infrastructure failure, treatment and planning, there are opportunities for the ATO to further develop testing exercises to assess and validate the BCM processes to effectively restore services from critical infrastructure system failures, and in a timely manner.

Business continuity strategies for stakeholders

3.36 In his messaging to Senate Estimates and other forums, the Commissioner of Taxation highlighted the importance of stakeholders[55] having their own business continuity arrangements that would help to improve the resilience of the entire tax and superannuation system.[56]

3.37 The ATO's Superannuation business service line has presented to the Superstream Industry Engagement Forum, and met with two peak forums[57] to assist them in understanding their business continuity strategies and improve the resilience of their superannuation systems. In these meetings, all parties agreed to establish a joint ATO–Industry Continuity Plan.

3.38 The ATO has also presented at tax agent forums to address concerns and provide updates on the ATO's initiatives to improve the availability and resilience of infrastructure and services, particularly during Tax Time. The ATO advised that it will shortly commence education initiatives for the tax agent community and software providers in response to stakeholder feedback. The ATO has also prepared a business continuity information sheet, with examples for small businesses to assist them in improving their own business continuity strategies.

3.39 The Australian Public Service BCM Community of Practice is a forum for government entities to share insights and resources relating to business continuity practices. Currently the Chair of the forum is an ATO Executive. Meetings are held monthly, and individuals offer coaching and mentoring. In addition to these meetings, the ATO's BCM team regularly meet with other agencies to provide insights and share lessons learned.

Has the ATO improved stakeholder communications?

The ATO has updated its communication strategy with a greater focus on providing relevant and useful information to internal and external stakeholders, using multiple channels, during system failures and unscheduled outages. The ATO has examined options to clearly communicate information about the application of general waivers and discretions in particular circumstances but has not resolved an approach—this recommendation is being implemented, and the other recommendation from this theme has been implemented.

Stakeholder communications following system failures and scheduled outages

3.40 The ATO has updated its communication strategy during system failures and unscheduled outages. In response to stakeholder feedback following the December 2016 and February 2017 incidents, the ATO examined its communication strategies and channels of communication during the system failures.

[55] The ATO identify key stakeholders as the superannuation industry, tax agents, software providers and other Australian Public Service entities.

[56] Senate Economics Legislation Committee Hansard, 30 May 2017, p. 14.

[57] The two bodies are: Association of Superannuation Funds of Australia Services Committee Executive; and the Gateway Network Governance Body.

3.41 The ATO advised the ANAO that it is addressing the feedback by developing ways to tailor the content of the communications based on describing what is happening and/or being done, and how that will directly affect different stakeholders. Specific actions undertaken include:

- an update of the ATO Systems Incidents Response Communications Strategy Overview;
- a new IT Systems Incidents Communication Process Map; and
- developing specific communication strategies for different stakeholder groups including tax professionals, superannuation funds, digital service providers, other government agencies, and for Tax Time 2017.

3.42 These activities provide a model for communication regarding system failures and scheduled outages. The ATO has specified stakeholder groups, channels for communication, content of messages, internal responsibilities and a process to follow in the event of severe outages. Information about systems failures available on the ATO website is consistent with the model.

3.43 The ATO's updated communication strategy has not yet been applied, as that will only occur when a major system outage occurs. There are opportunities for the ATO to further develop the communications strategy and increase its effectiveness in the event of a critical infrastructure and systems failure, including using its existing stakeholder forums to confirm that the proposed approaches align with the perspectives of stakeholders.

Communications about waivers and discretions

3.44 The ATO has committed publicly to ensuring that tax practitioners and taxpayers will not be disadvantaged by the impacts of its system issues during Tax Time 2017 and in future.[58] The ATO advised the ANAO that it continues to consider the best options for improving how to communicate about the application of general waivers and discretions to particular circumstances.

[58] Australian Taxation Office, 'Certainty for stakeholders who rely on ATO systems', media release, Canberra, 12 July 2017.

4. Service commitments and outage tolerances

Areas examined

The ANAO assessed if the ATO had established and met service commitments relating to the availability of ICT systems. The ANAO also assessed if system outage tolerances are included in service measures and service level agreements with contracted ICT service providers.

Conclusion

The ATO does not have service commitments specifically relating to the availability of ICT systems but does specify system outage tolerances in its major contracts with ICT service providers. To monitor the impact of ICT service outages on satisfaction with its services, the ATO should develop service standards that are aligned with system outage tolerances in its contracts with ICT service providers.

Areas for improvement

The ANAO made two recommendations aimed at determining the level of availability of services to include in service standards (paragraph 4.12), and aligning service measurement across major ICT service contracts (paragraph 4.29).

Introduction

4.1 As discussed in Chapter 1, public reaction to the outages and the ATO's response indicate a possible gap between external stakeholder expectations and the ATO's service offering. The differences involve two key questions:

- in what circumstances can services be reasonably disrupted without notice; and
- what is a reasonable duration for restoring services in the event of an outage?

4.2 In respect of the first question, system failures and unexpected outages occur for a variety of reasons, and cannot be completely eliminated. Decisions will always have to be made about the level of investment in ICT systems and standard of functionality achieved, including availability and reliability of services. If outages are consistent with decisions made regarding standards of functionality and consistent with an organisation's desired risk profile, then outages are part of reasonable management decisions. Outages may be part of a controlled process to prevent more widespread or severe problems.

4.3 In relation to the second question, time taken to return systems to operational status can be controlled by the design and implementation of specific recovery processes. To the extent that the system has operated as designed, including the implementation of recovery and restoration procedures, system failures and unscheduled outages cannot be regarded as management failures. An assessment of the management of system outages needs to focus on an organisation's business continuity management processes, including planning and implementation.

4.4 The severity and impact of system failures and outages also need to be included in change management processes. If appropriate, an organisational assessment should be made of the basis for management decisions regarding the risk profile of an enterprise ICT solution. In cases where users report significant disruption to their work, it is appropriate for an organisation to reassess its perspective on acceptable levels of service outage and consider whether to establish or amend desired levels of performance, including standards, measures and targets.

Has the ATO established and met service commitments?

The ATO does not have clear service commitments relating to the availability of ICT systems. There are no explicit measures for ICT service availability and existing service commitments have only broad application—through survey questions about ease of accessing services and information, and doing business with the ATO, and measures of timeliness in processing lodgements. Accordingly, the ATO has not broadly monitored the impact of ICT service outages on satisfaction with its services.

4.5 Service commitments are publicly stated standards for services. They take a variety of forms and differ between entities. Service commitments enable entities to set expectations and support accountability.

4.6 The ATO sets out service commitments on its website, described as 'the five key elements you wanted us to focus on because they were important to you'. These are listed as: helpful and accurate; easy to deal with; timely; keep me informed; and professional.[59] The ATO has defined assessment indicators and performance measures for each of these five elements. Table 4.1 presents the assessment indicators and performance measures that are most likely to reflect online service outages, and their assessed performance. The table shows that the ATO has met its targets for these indicators over the past three years.[60]

Table 4.1: ATO performance against relevant measures, 2014–15 to 2016–17

Assessment indicator	Performance measure	2014–15	2015–16	2016–17[a]
The ATO makes it easy for me to access the services and information I need.	People surveyed agreed that the ATO makes it easy to access services and information.	70 per cent	78 per cent	75 per cent
It was easy to do business with the ATO.	People surveyed agreed that the ATO was easy to do business with.	66 per cent	72 per cent	69 per cent
Process my lodgements within timeframes.	94 per cent of individual and non-individual electronic tax returns are finalised in 12 business days (applies to current year tax returns only)	94 per cent	98 per cent	99 per cent as at 31 August 2017
	94 per cent of electronic activity statements are finalised in 12 business days.	100 per cent	100 per cent	100 per cent as at 31 August 2017
	90 per cent of electronic amendments are finalised in 20 business days.	94 per cent	94 per cent	95 per cent as at 31 July 2017

[59] Available from <https://www.ato.gov.au/about-ato/access,-accountability-and-reporting/our-commitments-to-service/current-year-commitments-to-service/> [accessed 12 September 2017].

[60] Targets exist for the lodgement processing indicators but not for survey questions.

Assessment indicator	Performance measure	2014–15	2015–16	2016–17[a]
	93 per cent of Australian residents' ABR registrations are finalised in 20 days.	97 per cent	98 per cent	99 per cent
	93 per cent of electronic Commissioner of Taxation registrations are finalised in 20 business days.[b]	97 per cent	97 per cent	97 per cent as at 31 July 2017

Note a: Unless stated otherwise, the performance measure is as at 30 June 2017.

Note b: In 2014–15 the target for this performance measure was 93 per cent of Commissioner of Taxation registrations finalised in 28 calendar days.

Source: ANAO, from ATO data.

4.7 The assessment indicators are helpful in gauging stakeholders' feedback on the ease of access to services and information, and whether the ATO was easy to do business with. However, the indicators are not stated in a manner to provide meaningful feedback on the impact on stakeholders if services are unavailable due to system failures, and planned and unscheduled outages. For example, the indicator measuring the timeliness to process electronic lodgements is based on the time elapsed after the ATO receives the lodgements—it excludes the time lost by the user to gain online access or to submit their lodgements due to system outages.[61] While respondents may consider online availability in answering questions about ease of access to services and information, and whether the ATO was easy to do business with, the importance of system outages is not evident from those responses.[62]

4.8 No assessment indicators or performance measures explicit to online services are included in the ATO's statement of service commitments, corporate plan, portfolio budget statements or annual reports. There are no quantitative measures at a corporate level to assess service availability.

4.9 The *ATO corporate plan 2016–17*, however, does acknowledge stakeholder expectations to service commitments:

> Community and client expectations about the services and products we offer continue to change as developments in technology create new ways to interact. As we harness these technologies, we work to stay in tune with client and stakeholder needs and expectations, and understand the experience they expect when interacting with us. We then co-design and develop the services we offer accordingly.[63]

[61] This measurement does not incorporate the key performance indicators of completeness contained in the Digital Service Standard (see paragraph 1.9), which measures the percentage of completed transactions of commenced transactions.

[62] The ATO has advised the ANAO that it has raised the issue of systems outages and received feedback about them in the context of stakeholder forums, particularly the *Tax Practitioner Stewardship Group, Superannuation Industry Stewardship Group* and *Software Developers Strategic Working Group.* However, the ANAO reviewed records of meetings provided by ATO and did not identify consultation on systems outages.

[63] Australian Taxation Office, *ATO Corporate plan 2016–17*, p. 11. Available from <https://www.ato.gov.au/about-ato/about-us/in-detail/strategic-direction/ATO-corporate-plan-2016-17/> [accessed 6 October 2017].

4.10 The ATO corporate plan 2016–17 reports the ATO's enterprise risks. One enterprise risk refers to standards of systems performance—Risk 6: Our information and communications technology (ICT) systems fail to perform consistently to the standard required. The ATO corporate plan 2016–17 states in relation to managing this risk:

> Our ICT systems need to be able to: handle the demands of new online services and the integrated nature of whole-of-government technologies … As the community embraces new and emerging technologies and communication channels, the demands for security, convenience, and 24/7performance of our systems mount.[64]

4.11 These statements indicate recognition of expectations of high availability of online services, but that the ATO has not yet either specified levels of online service availability for users or how to best reflect availability in service standards.

Recommendation no.2

4.12 The ATO determines the level of availability of services associated with ICT systems to include in service standard(s) and subsequently reports performance against those standard(s).

Australian Taxation Office response: *Agreed.*

4.13 *The ATO already has a range of service commitments relating to its performance as a tax administration. For example, we have commitments related to how quickly general telephone calls will be answered during Tax Time and commitments on how quickly electronic activity statements will be finalised. The identification of service commitments in relation to the availability of services associated with ICT systems would be on the same footing as these other service commitments.*

4.14 *A range of mechanisms already exist that hold the ATO accountable for their performance against these service commitments. These include the Tax and Revenue Standing Committee's annual enquiry into the ATO's Annual Report and other Parliamentary scrutiny (for example, Senate Estimates). As part of the ATO's commitment to transparency and keeping the public informed, it publishes performance updates against its service commitments monthly on ato.gov.au.*

Are system outage tolerances included in service level agreements?

Outage tolerances are included as service measures in service level agreements for the major ICT service contracts, and equate to high availability of services and systems. Tolerances have been internally reported as largely met in recent years, although the recent system failures have been excluded, which means performance has been overstated for 2016–17. With the major ICT service contracts scheduled to be renegotiated in 2018, the ATO has an opportunity to align service measures across its ICT contracts and also align service standards with the outage tolerances in its ICT service contracts. In this light, the ATO could strengthen service measures in its cloud computing service contracts.

[64] ibid., p. 13.

Specification of tolerances in major ICT service contracts

4.15 The service contracts between the ATO and contracted ICT service providers specify tolerances for system failures and unscheduled outages. For example, the Centralised Computing Services contract (managed by DXC) is for services and assets related to midrange, mainframe, storage, data warehouse and security, with agreed tolerance indicators shown in Table 4.2.

Table 4.2: Key tolerances for Centralised Computing Services, and reported performance for 2016–17

Tolerance indicator	Performance standard per month	Reported performance for 2016–17[a]
Lost business time for specified applications and systems		
Tier 3 systems	Less than 45 minutes	44 minutes
Tier 4 systems	Less than 90 minutes	18 minutes
Incident resolution time for Priority Levels 1 and 2		
Priority Level 1	92 per cent of incidents resolved within **four hours**	69.5 per cent
Priority Level 2	92 per cent of incidents resolved within **ten hours**	95 per cent

Note a: Actual performance is a calculated on annualised averages.

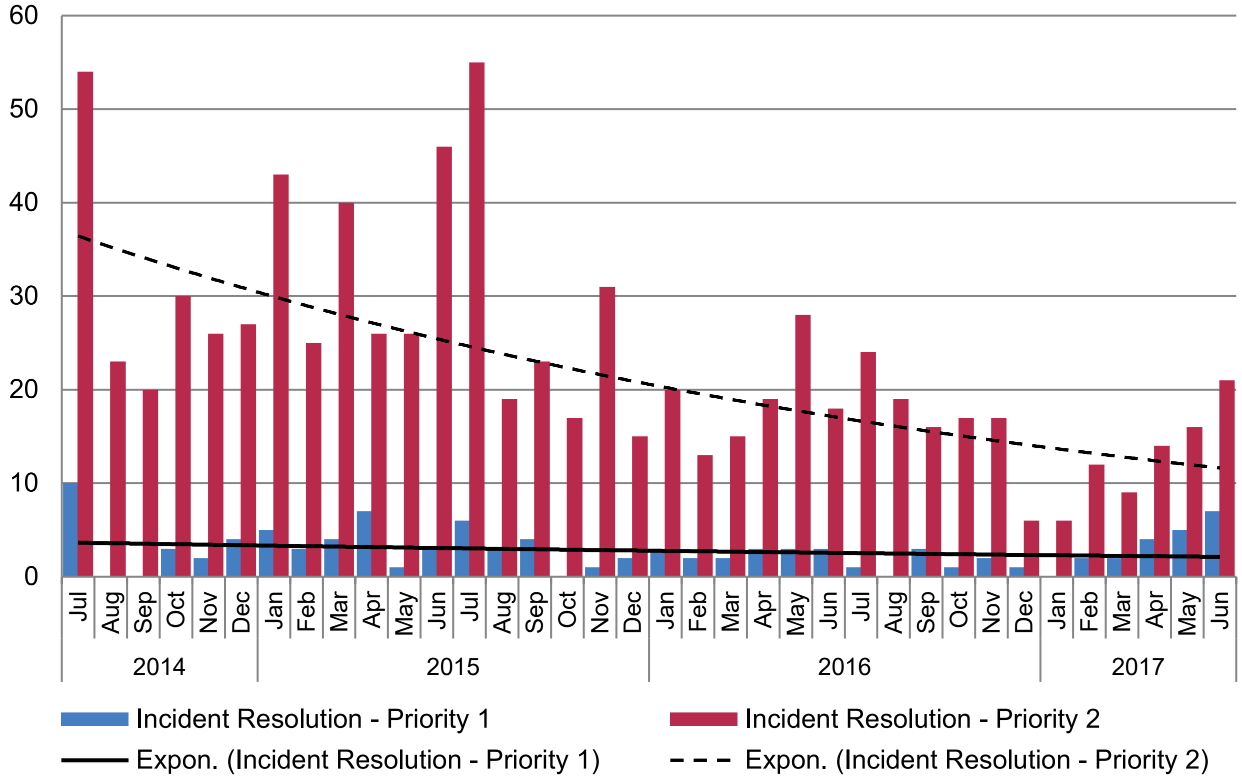
Source: ANAO, from ATO data.

4.16 The ANAO examined the ATO's annual performance assessments and the monthly performance scorecards for each service provider for the twelve month period from July 2016 to June 2017. All providers were recorded by the ATO as meeting all minimum performance requirements for reliability-related metrics.

4.17 The ANAO also analysed data on priority level 1 and 2 incidents from 2014–15 to 2016–17 to gauge the trend in system failures. Figure 4.1 illustrates incidents by priority by month with exponential trend lines. This analysis indicates that the total number of recorded priority incidents has reduced each year, indicating fewer system failures and unscheduled outages in 2017 than in previous years.[65]

[65] The total number of reported priority level 1 and 2 incidents in 2014–15 was 428 incidents; in 2015–16 was 305 incidents and in 2016–17 was 205 incidents.

Figure 4.1: Number of ICT priority level 1 and 2 incidents, 2014–15 to 2016–17



Source: ANAO analysis of ATO data.

4.18 The service measurement approach has identified few problems with service providers meeting agreed tolerance requirements, and the number of priority level 1 and 2 incidents is declining.

4.19 While the December 2016 and February 2017 system failures have been included in the measurement of ICT priority level 1 and 2 incidents[66], the impacts of the failures have been excluded from performance scorecard reporting and assessments. The Centralised Computing Services contract has excluded the impacts of the system failures—as the failures are addressed separately under a Deed of Resolution[67]—and these have not been captured elsewhere for inclusion in the performance assessments. Excluding these system failures has overstated the extent to which tolerance requirements were met in 2016–17. The ANAO considers that the system failures should be included for the purpose of reporting performance against specified tolerances.

4.20 The ATO advised that very little assurance checking is undertaken on the performance scorecards due to the level of automation and reliance on the contracted ICT service providers.[68]

[66] The ATO’s change management records capture the incident as a single Priority 1 event. The record remains in ‘open status’, implying the issue remains unresolved.

[67] The Deed of Resolution between the ATO and DXC Technology (discussed in Chapter 2) also has provisions to exclude the SAN incident from ongoing performance measures.

[68] *Ad hoc* checks are conducted, with a focus on excusable delay events. An excusable delay event is a request to exclude data from a performance measure on the basis that contributing factors were outside the service providers controls and not reflective of their commercial performance.

As discussed in paragraphs 3.28 and 3.29, Leidos was aware of continuing unresolved issues with the SAN arrays but did not report these issues to ATO executives. This is an example of under-reporting by a contractor, which the ATO had little visibility of in light of the lack of assurance over the performance assessment processes.

4.21 As discussed in paragraph 2.32, in 2017 the ATO conducted an internal audit of the contract and relationship with DXC, and whether any aspects of the arrangements exceeded ATO tolerances.[69] The audit concluded:

> From an operational and transactional perspective, no significant gaps or deficiencies were identified that need to be immediately addressed or which may have exposed the ATO to significant risks in the delivery of products or services under the Centralised Computing contract.
>
> Notwithstanding, a number of areas in relation to strategic management, both within Enterprise Solutions and Technology Group (EST)[70] and at the organisational level, have been identified where risks may exceed the ATO's tolerance, and therefore additional treatments are recommended … which should also be considered across the ATO's broader contract and project management environment.[71]

4.22 The ANAO notes that the ATO does not have measures at the corporate or strategic level to enable a confident assessment of whether risks exceed tolerances, as discussed in the first section of this chapter. Determining a service standard or equivalent corporate measure for ICT outages would support such a risk assessment. It is important that the service standards or equivalent measures are aligned with tolerances specified in contracts with ICT service providers.

Service measures in major ICT service contracts and cloud computing services

4.23 Tolerances are part of the broader performance framework and measures for the ATO's ICT contracts. The ANAO's examination of the major ICT contracts in place between the ATO and contracted ICT service providers identified three stages in the development of contractual relationships and service measurement.

- In 2008, the ATO commenced an ICT Sourcing Program that led to contracts for three separate groups of services, referred to as bundles. The bundles were for End-User Computing (contracted to Leidos), Managed Network Services (contracted to Optus), and Centralised Computing (contracted to DXC).
- In 2016, the ATO began to set up contracts for cloud computing services. It now has three separate contracts in place with Amazon Web Services[72], MacGov [73] and Azure.

[69] The ATO's Chief Internal Auditor and Chief Risk Officer undertook a review of arrangements with DXC, to identify any risks exceeding ATO's tolerance associated with delivery, management and oversight arrangements.

[70] EST is in the Chief Information Officer Group within ATO, and has responsibility for technology and architecture, service operations, digital service delivery and enterprise capability.

[71] Australian Taxation Office, *HPE Review: Products, Services and Relationships Report*, 14 July 2017, p. ii.

[72] The ATO entered into a contract with Amazon Web Services, Inc. on 16 December 2016. The contract was prepared by Amazon Web Services—as a standard contract—for 'services offers as provided by AWS or its affiliates for which customer registers via the AWS site.' There are no provisions for service measures and service levels that are specific and applicable for the ATO in its service commitment to deliver services.

- In 2017, the ATO and DXC agreed to remove the SAN services from the Centralised Computing contract and manage it under a separate Deed of Resolution.

4.24 The service measurement approaches vary considerably according to the stage of contract development, as shown in Table 4.3.

Table 4.3: Core elements of ATO's ICT service measures

Core elements of ATO's ICT service measures	Summary assessment for the three bundles of major ICT contracts	Summary assessment for the three cloud computing services
Service indicators		
Defined as: • key indicators and service requirements are identified. • indicators are quantified and measurable. • indicators are linked to service measures.	• Comprehensive set of indicators, consistent with specifications for contracted services.	• Included in MacGov contract only.
Service monitoring and reporting		
Defined as: • system performance is monitored and periodically reviewed. • the standard of service is reported and assessed against service indicators and critical deliverables.	• Monthly, quarterly and annual assessments—question mark regarding robustness of information presented for assessment.	• Not defined in any of the contracts.
Critical system deliverables		
Defined as: • essential system components for the delivery of IT service are defined, and supported by documented actions and tolerances are set. • certified by an independent party.	• specified for each contract, but appear not to be updated and information on them is not included in regular performance reports.	• Included in the MacGov contract only.
Commercial assessments		
Defined as: • commercial arrangements with contracted service providers are periodically reviewed and assessed based on the reporting of system performance. • adjustments to the contracted service providers' payments are based on performance levels.	• Conducted annually (except for Active Directory) based on results of performance assessments—question mark as for service monitoring and reporting.	• Not provided for in any contract.

Source: ANAO analysis.

[73] The ATO entered into a contract with Macquarie Telecom Pty Ltd (MacGov) on 16 May 2016. These services include establishment of connectivity through dark fibre services, encryption devices and licences, firewalls and a self-managed virtual data centre. Following the SAN outages in December 2016, the ATO expanded the scope of services to include backup as risk mitigation for Tax Time 2017 testing.

4.25 The three major bundles of ICT contracts incorporated a Performance Framework in their contractual service level agreements. Consistent with that framework, the service measures were generally well specified across the categories of: service indicators; service monitoring and reporting; critical system deliverables; and commercial assessments. The measures have been adjusted periodically with the aim of ensuring they remain relevant to achievement of corporate objectives. Notwithstanding these adjustments, the performance measures have their origins in contracts that were agreed to almost ten years ago—at a time when the ATO's stakeholders were less reliant on online services and high availability.

4.26 The Performance Framework, as discussed above, is not applied to cloud computing services, which do not include many of the service measures in the major ICT contracts. The Deed of Resolution between the ATO and DXC to manage the SAN outages also does not include many of the service measures in the major ICT contracts.

4.27 The ATO's ICT infrastructure continues to be modified in response to demands for online services, and the availability of new technologies to support digital platforms and address risks and issues with legacy ICT systems. Use of new technologies is resulting in the ATO entering into different types of contracts with service providers. In 2018, the three bundles of major ICT contracts will be due for renewal. The combination of these events provides the ATO with an opportunity to reassess its ICT service measurement approach, and where possible implement common approaches, at least in terms of reflecting tolerances that align with the ICT outage service standards that the ATO has committed to develop.[74] Such an approach would support the ATO in its efforts to use digital technology and online services effectively and efficiently in the administration of the taxation and superannuation systems

4.28 Two particular matters to consider are:

- revise the service measurements applying to the Amazon Web Services cloud service contract that does not include service level provisions. This contract exposes the ATO to contractual and operational risks in the absence of measurable service levels.
- to the extent possible, align service measurements arrangements for services sourced through ATO procurement processes, and those obtained through whole-of-government and shared ICT procurement options.

[74] A consistent and standardised agreement is useful to simplify management and reporting of delivered services—but also critically the agreements need to support effective ICT services and variations between contractual specifications.

Recommendation no.3

4.29 The ATO includes tolerances in its ICT service contracts that align with service standards associated with ICT systems, where possible.

Australian Taxation Office response: *Agreed.*

4.30 Once service commitments have been agreed by the ATO Executive as per recommendation 2, the ATO will review tolerances, which are already included in our major ICT service contracts. Any changes to performance will need to be balanced against the cost of delivering to new availability commitments.

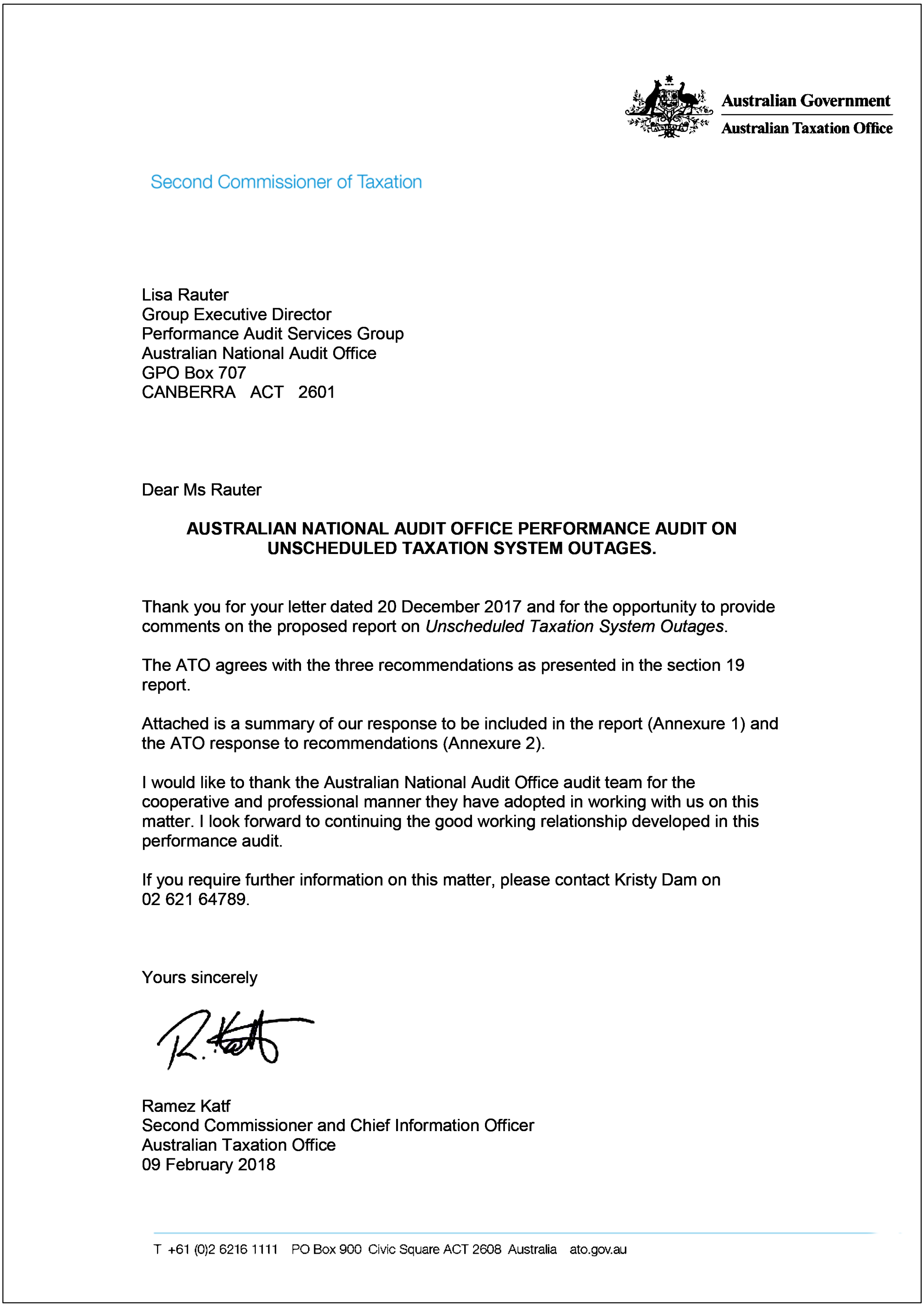
Grant Hehir

Grant Hehir
Auditor-General

Canberra ACT
20 February 2018

Appendices

Appendix 1 Response from the Australian Taxation Office



Australian Government
Australian Taxation Office

Second Commissioner of Taxation

Lisa Rauter
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Ms Rauter

AUSTRALIAN NATIONAL AUDIT OFFICE PERFORMANCE AUDIT ON UNSCHEDULED TAXATION SYSTEM OUTAGES.

Thank you for your letter dated 20 December 2017 and for the opportunity to provide comments on the proposed report on *Unscheduled Taxation System Outages*.

The ATO agrees with the three recommendations as presented in the section 19 report.

Attached is a summary of our response to be included in the report (Annexure 1) and the ATO response to recommendations (Annexure 2).

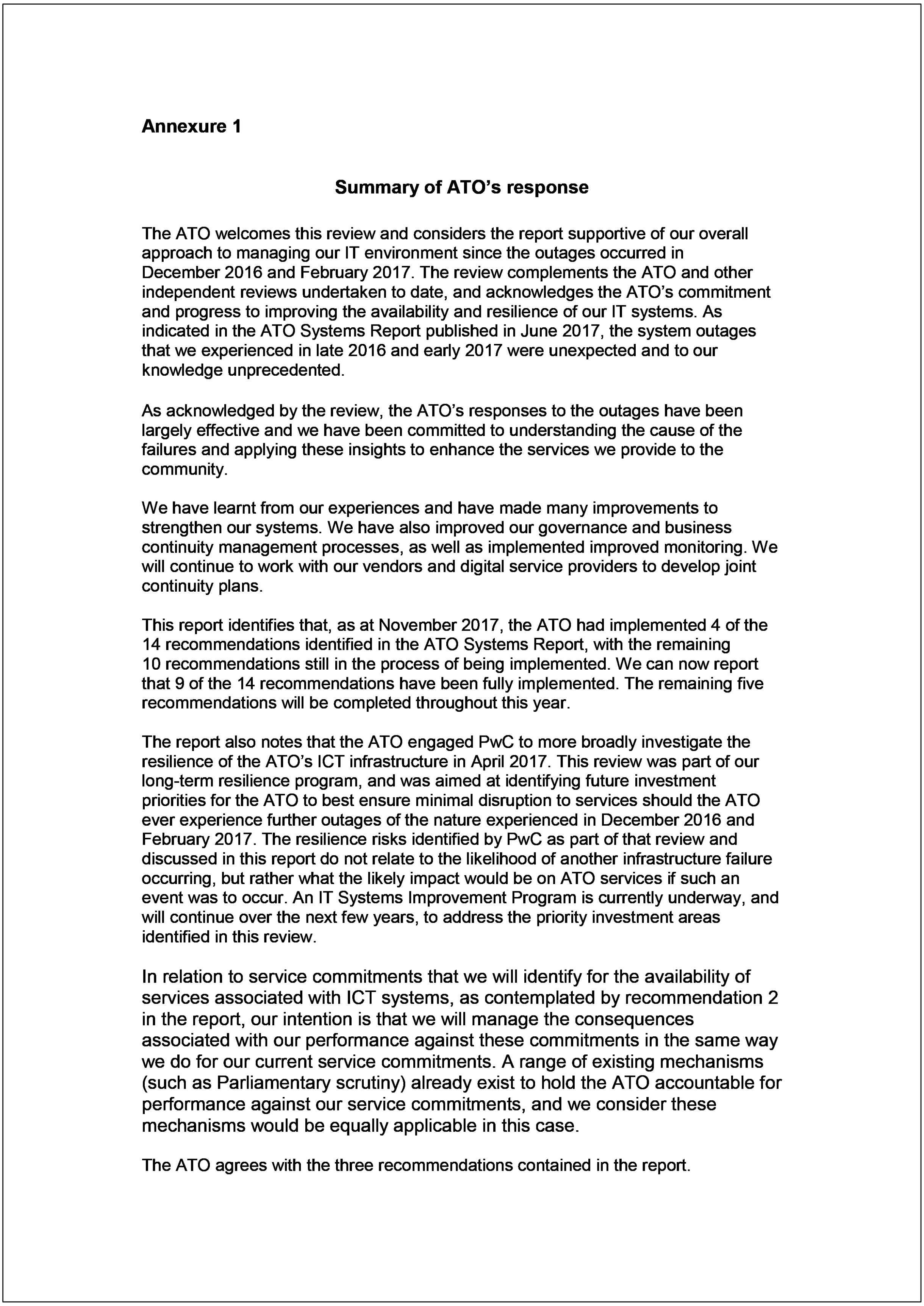
I would like to thank the Australian National Audit Office audit team for the cooperative and professional manner they have adopted in working with us on this matter. I look forward to continuing the good working relationship developed in this performance audit.

If you require further information on this matter, please contact Kristy Dam on 02 621 64789.

Yours sincerely

Ramez Katf
Second Commissioner and Chief Information Officer
Australian Taxation Office
09 February 2018

T +61 (0)2 6216 1111 PO Box 900 Civic Square ACT 2608 Australia ato.gov.au



Annexure 1

Summary of ATO's response

The ATO welcomes this review and considers the report supportive of our overall approach to managing our IT environment since the outages occurred in December 2016 and February 2017. The review complements the ATO and other independent reviews undertaken to date, and acknowledges the ATO's commitment and progress to improving the availability and resilience of our IT systems. As indicated in the ATO Systems Report published in June 2017, the system outages that we experienced in late 2016 and early 2017 were unexpected and to our knowledge unprecedented.

As acknowledged by the review, the ATO's responses to the outages have been largely effective and we have been committed to understanding the cause of the failures and applying these insights to enhance the services we provide to the community.

We have learnt from our experiences and have made many improvements to strengthen our systems. We have also improved our governance and business continuity management processes, as well as implemented improved monitoring. We will continue to work with our vendors and digital service providers to develop joint continuity plans.

This report identifies that, as at November 2017, the ATO had implemented 4 of the 14 recommendations identified in the ATO Systems Report, with the remaining 10 recommendations still in the process of being implemented. We can now report that 9 of the 14 recommendations have been fully implemented. The remaining five recommendations will be completed throughout this year.

The report also notes that the ATO engaged PwC to more broadly investigate the resilience of the ATO's ICT infrastructure in April 2017. This review was part of our long-term resilience program, and was aimed at identifying future investment priorities for the ATO to best ensure minimal disruption to services should the ATO ever experience further outages of the nature experienced in December 2016 and February 2017. The resilience risks identified by PwC as part of that review and discussed in this report do not relate to the likelihood of another infrastructure failure occurring, but rather what the likely impact would be on ATO services if such an event was to occur. An IT Systems Improvement Program is currently underway, and will continue over the next few years, to address the priority investment areas identified in this review.

In relation to service commitments that we will identify for the availability of services associated with ICT systems, as contemplated by recommendation 2 in the report, our intention is that we will manage the consequences associated with our performance against these commitments in the same way we do for our current service commitments. A range of existing mechanisms (such as Parliamentary scrutiny) already exist to hold the ATO accountable for performance against our service commitments, and we consider these mechanisms would be equally applicable in this case.

The ATO agrees with the three recommendations contained in the report.

Appendix 2 Preliminary technical assessment and steps taken

In late February 2017, DXC provided the ATO with a formal briefing on the December 2016 and February 2017 system failures.

System failure in December 2016:

- At 2300 on 11 December 2016, errors occurred on a Serial Attached SCSI (SAS) data path. The data path consists of a data transfer initiating device, a cable, expanders for connections to more than one receiving device, and receiving devices. These errors degraded the operation of Solid State Drives (SSDs) in two drive cages (enclosures/casings).
- At 0100 on 12 December 2016, an investigating engineer found multiple 3PAR volumes [drives or drive segments in the 3PAR server] in a preserved (non-functioning) state. These volumes were dependent upon the SSDs that were in a degraded state due to the connection/data path errors. The engineer 'power cycled' (turned off and on) the SSDs both by command and by pulling them out of their slots and putting them back in.
- This reset procedure was performed on 21 drives—12 of which did not restart and reported a 'destructive error event'. The 12 failed drives were executing a port (self)-recovery subroutine at the time of the power reset.
- A senior engineer reviewed event logs in the early morning and identified the destructive error event message. DXC attributed this late detection to the way in which the error message is generated: not when the drive is reset but when a routine tries to send or draw data from it. The initial investigating engineer had wrongly concluded that the power cycling had worked.
- The 12 failed SSDs were deactivated.

System failure in February 2017:

- At around 2200 on 1 February 2017, DXC technicians were replacing data path cables as part of a plan to address the problem that caused the 12 December outage. A faulty new connection led a node [disk] controller to restart unexpectedly.
- At about 0115 on 2 February 2017, a decision was taken to replace the node controller, but the replacement failed to operate successfully and was shutdown. This shutdown caused another node, running a routine with the shutdown node, to go into 'panic mode' and close down. DXC noted that 3PAR clusters are designed to operate in a N minus 1 mode (with N being the number of nodes, in this case 9 in total) and that the loss of two nodes causes a shutdown of all nodes to preserve data.
- A 'power fail recovery' was executed to restore the cluster, but by 1500 on 3 February 2017 it was realised that the procedure was taking too long due to the failed state of the SSDs from the 12 December 2016 incident.

The Performance Framework objectives for ICT system services are common to all service providers. They are: supporting business change; partnering for outcomes; ongoing Business value; sustainable business.