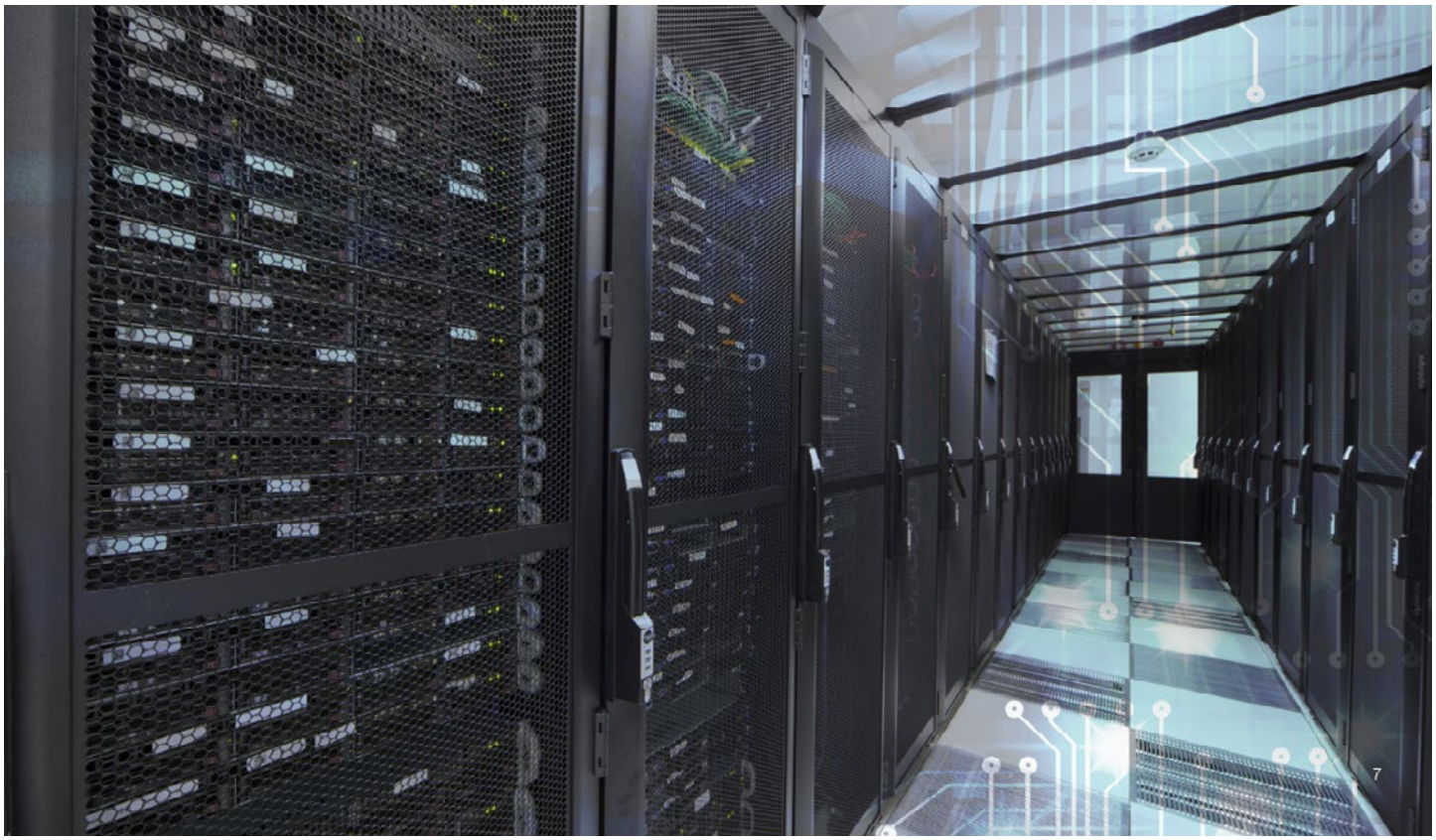
June 2017

ATO systems report



JS 39322

Australian Government
Australian Taxation Office

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information in this publication and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we must still apply the law correctly. If that means you owe us money, we must ask you to pay it but we will not charge you a penalty. Also, if you acted reasonably and in good faith we will not charge you interest.

If you make an honest mistake in trying to follow our information in this publication and you owe us money as a result, we will not charge you a penalty. However, we will ask you to pay the money, and we may also charge you interest. If correcting the mistake means we owe you money, we will pay it to you. We will also pay you any interest you are entitled to.

If you feel that this publication does not fully cover your circumstances, or you are unsure how it applies to you, you can seek further assistance from us.

We regularly revise our publications to take account of any changes to the law, so make sure that you have the latest information. If you are unsure, you can check for more recent information on our website at **ato.gov.au** or contact us.

This publication was current at **June 2017**.

Published by

Australian Taxation Office
Canberra
June 2017

JS 39322

Commissioner's foreword

It almost goes without saying that harnessing technology and using digital channels is the way of the future. Technology offers our clients, agents and the ATO great efficiencies with automation of simpler tasks, freeing us up to work on things of greater value.

In the future, the vast majority of taxpayers will use our digital services to send and receive information and payments, and to complete transactions in real time.

We acknowledge that these new ways of working bring their own challenges and to maintain the trust and confidence of the community, we need to ensure the technology upon which we, our partners and our clients depend is secure and reliable.

The system outages that we experienced in December 2016 and February 2017 were unexpected and to our knowledge unprecedented. I can also say that in no way did our new products and services under our reinvention program cause the outages.

Once the December outage occurred, we in the ATO and our contract service provider, Hewlett Packard Enterprises (HPE) acted immediately, with HPE making available resources from across the globe. HPE staff cooperated and communicated openly with us, working tirelessly around the clock, including through the Christmas period, to ensure our systems and services were restored as quickly as possible.

This report explains what happened to our IT systems, the impacts on our stakeholders, the ATO responses, and what we are doing to improve our services in the future.

We are very mindful of the disruption that the outages caused the community and our key stakeholders – tax practitioners, the superannuation industry and software providers. I apologise again for the inconvenience that has been experienced.

No taxpayer data has been lost or compromised as a result of the outages and government revenue for 2016–17 has not been impacted. Further to this, all refunds were paid inside our service standards and any affected taxpayers were automatically allowed additional time to lodge or make payments to us.

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.

With these measures in place, we are confident that when Tax Time 2017 commences on 1 July 2017, we can match the experience of Tax Time 2016 and taxpayers will be able to lodge their returns and receive their refunds.

Our contract service providers, HPE and DXC Technology, continue their forensic investigations into the root causes of these outages, including laboratory testing of decommissioned equipment. If these tests suggest significantly different issues we will provide an addendum to this report.

In developing this report, we have drawn from numerous sources, including feedback from clients and stakeholders, technical analysis from our service providers and a separate independent review. In addition, we conducted a review to draw lessons from the response to these incidents and to improve our services to the people and enterprises of Australia and our partners.

This report is based on our current understanding of the issues related to the outages as at 8 June 2017.

Chris Jordan AO
Commissioner of Taxation

Executive summary

To provide myriad services to over 12 million clients, and partners, and to hold data securely, the Australian Taxation Office (ATO) operates a complex computing platform. This platform is managed by a combination of ATO staff with IT expertise and contracted service providers. On 12 December 2016, and again on 2 February 2017, there were ATO computing systems outages (systems outages) that impacted our services to the Australian community following issues with part of our data storage system.

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 on by the ATO, and they have relevance across the tax and superannuation systems, and for others who use or rely on complex IT systems.

Late on 11 and early on 12 December 2016, one of the ATO's Storage Area Networks (SAN) operated and maintained by Hewlett Packard Enterprises (HPE) in a storage facility in Sydney, failed. This SAN failure resulted in a systems outage, causing the majority of the ATO's online services to become unavailable, with significant disruption to our clients and stakeholders.

Whilst HPE and DXC Technology continue to investigate the issues related to this outage, our current findings indicate:

- In balancing performance, stability, resilience and cost factors, when designing the Sydney SAN, there was a relative focus on performance. Some resilience features were incorporated into this design, but did not contemplate or anticipate the specific combination of events that resulted in these incidents, which to our knowledge are unprecedented.
- Some in-built SAN monitoring and resilience features were not enabled, including a facility to better report alerts back to HPE.
- The outage experienced in December 2016 resulted from the compound impact of:
  - multiple SAN component failures on the Sydney SAN, which included failures associated with stressed fibre optic cabling
  - subsequent unsuccessful attempts for the system to auto-recover in response to the component failures (consequently the SAN was unable to provide read/write services to the applications it supported)
  - control, management and monitoring systems being placed 'in-band', that is, these systems relied on the same data pathways as the production systems that were supporting impacted services.
- The outage commenced around 12.40am on 12 December 2016 (that is, data volumes had entered a preserved state to protect data integrity and were therefore not available to support ATO applications and services), and by 3.35am on 12 December 2016 a significant number of data volumes were in this state (455 out of 3,063).
- The firmware supporting impacted disk drives in the SAN prevented those drives from re-booting.
- Despite having met ATO specified conditions for categorisation as a Priority 1 incident at this time (3.35am) service provider logs indicated the incident was not escalated to this level until around 7.00am that morning.
- The fact that system management, configuration, monitoring, and data recovery systems that were relying on the SAN also experienced outage extended the recovery process for some applications.
- In addition, the impact of pre-incident design and build decisions were material in extending the time to recover data and bring production and supporting systems online.

At this stage of the investigation, we consider that stressed fibre optic cabling issues were a major contributor to this outage.

It is important to reiterate that our systems were not subject to external attack. In addition, we have confirmed that we have found no evidence of any lost taxpayer data as a result of these outages.

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 HPE 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.

The second outage on 2 February 2017 followed further remedial work by HPE on these SAN fibre optic cables. Unfortunately, during one cable replacement exercise, we were informed that data cards attached to the SAN had been dislodged. This caused the 3PAR SAN to act in a similar way to that noted during the December outage. This included unsuccessful steps to automatically remediate, followed by a systems shut-down to preserve data integrity. HPE communicated this Priority 1 incident to us immediately.

As a result, HPE and the ATO monitored these cables around the clock, until they were comprehensively replaced between 23 and 26 March 2017. We have since been advised that SAN alerts ceased completely once the new fibre optic cables were installed.

The ATO successfully invoked business continuity management arrangements following these outages to inform stakeholders and to restore services. Once aware of the impact of these outages, the ATO and our contract service providers made available local and global staff to work together on restoration activities.

Following restoration, our priority was to address any disadvantage suffered by our clients. Most of these issues were dealt with using discretions and remedies available to us under the tax and superannuation laws, including extensions of time and adjustments to interest/penalty charges. We have also applied administrative concessions where due to the unavailability of services, taxpayers were unable to access the early payment discount for HECS/HELP debt. For other cases of disadvantage, we have a well-established process to consider applications for compensation under the Commonwealth's *Scheme for Compensation for Detriment caused by Defective Administration* (the CDDA Scheme).

The review and analysis of these IT incidents has been very thorough and is ongoing. We have:

- sought feedback from clients and stakeholders to understand their experiences
- taken account of the current findings of a root cause review from HPE which will ultimately involve detailed forensic testing of their equipment including cabling and their SAN
- commissioned independent experts, including PricewaterhouseCoopers (PwC) and the CTO Group, to provide us with detailed technical advice
- conducted our own review of these events to test and improve upon our procedures to provide better services to our clients in the future.

We received feedback from key stakeholders and the broader public, in relation to our response to the incident. In general it was found that our communications and client engagement was largely positive with some suggested improvement regarding consistency of messaging and terminology. There was also feedback that our response to incidents of this nature should consider the broader tax and super ecosystem and not just the services that we directly manage.

The observations and recommended improvements in this report solely reflect our views based on the range of sources outlined above.

The lessons from these IT incidents are already being implemented in the ATO. Our storage system has been rebuilt to world class levels of both performance and resilience. Our reflections on these incidents will help shape our future IT sourcing and activities to:

- support better services
- engage in new technology to enhance performance and resilience (for example, the use of the cloud environment)
- be as cost effective as possible.

Recommended improvements

Reflecting on the independent recommendations contained in the PwC report and feedback we received from key stakeholders and the community as part of our own post incident review, we have identified 14 key areas for improvement. These recommended improvements fall into the following five general themes:

1. Principles informing the ATO's IT design
2. Correcting the identified faults
3. Enhancing ATO capability to support infrastructure design and IT governance
4. Incident responses for the ATO and the wider tax system
5. Managing communication and business resumption with stakeholders.

We are committing ourselves to address each of these areas for improvement. In a number of cases, we have already delivered these improvements or are well progressed in doing so.

Theme 1 – Principles informing the ATO's IT design

Rec 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.

Rec 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 faults

Rec 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.

Rec 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.

Rec 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.

Rec 2.4 – Review and risk assess ATO infrastructure to improve resilience and mitigate the impact of a complete data storage failure whist 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 IT governance

Rec 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.

Rec 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 design capability to better ensure the build of IT systems by contractors is compliant with approved designs.

Rec 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

Rec 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 with the appropriate balance of performance, stability, resilience and cost factors.

Rec 4.2 – Consolidate, streamline, update, and simplify existing business continuity management documentation to clearly articulate the relationship between, and respective accountability for, business continuity, disaster recovery, and resilience planning.

Rec 4.3 – The ATO should assist key stakeholders to understand our business continuity strategies in order for them to improve their own continuity strategies. In turn, 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

Rec 5.1 – In the event of an unscheduled, high impact, disruption to ATO services, to support the transparency and regularity of ATO communications, we need to improve key stakeholder communications, ensuring they are tailored to each particular stakeholder's experience.

Rec 5.2 – Where ATO systems outages impact on a stakeholder's business model or their forward planning, we 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.

Contents

What happened and why

The ATO's IT framework – pre-incident conditions and factors

Consistent with large business organisations and government departments, the ATO runs a complex computing system to engage with clients, provide digital services and to hold data securely. This computing system includes service providers on contract that offer particular expertise and cost savings, including Hewlett Packard Enterprises (HPE).

In December 2010 we signed a five-year contract with HPE for Centralised Computing (CC) services. After a stabilisation period to ensure the proper transition from an earlier arrangement, the five-year contract term commenced in July 2013[1]. The scope of the CC services offered to the ATO includes our large processing systems (systems of record), systems of client engagement (portals), data warehouse and internet gateway services.

At the beginning of 2015, a sourcing, design and implementation process commenced in relation to the ATO's storage area network (SAN) solution. HPE recommended the installation of a state-of-the-art HPE 3PAR SAN[2] to replace the existing EMC Corporation SAN. This was on the basis that the 3PAR solution:

- created a more flexible storage environment that would better optimise costs
- was supported by HPE operating procedures and technical expertise.

This was agreed to by us, and the installation of the new 3PAR SAN was completed in November 2015.

We engaged HPE to provide turn-key[3] IT solutions, whereby HPE designs, owns and operates computing infrastructure and provides services to the required ATO standard. Under this turn-key operation, ATO IT staff have no direct access to the SAN technology operated by HPE. Instead, we rely upon HPE to provide a full service. To enhance and coordinate the work of our IT contractors, the ATO also contracted with Leidos Holdings, Inc. (Leidos) as service integrator. Leidos operates a virtual dashboard over myriad ATO IT systems, and provides a problem management process should issues arise with parts of our IT infrastructure.

The storage solution provided by HPE to the ATO comprised a primary 3PAR SAN in Sydney with a backup 3PAR SAN in Western Sydney. Consistent with good practice, data from one SAN is replicated to the other on a regular basis. Procedures were also in place to provide manual fail-over for selected applications in the event of a failure. Full automated fail-over for the entire suite of applications and services in the event of a complete SAN failure in Sydney was not part of the storage solution for the SAN. The cost of automatic fail-over systems, as they exist in some areas of critical infrastructure or in large financial institutions, is very high.

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. Specifically since May 2016, at least 77 events related to components that were observed to fail in the December 2016 incident were logged in our incident resolution tool managed by Leidos. In addition at least 159 alerts were recorded in SAN device monitoring and management logs (SNMP logs).

Some actions had been initiated by Leidos and HPE in response to these indicators, including:

- collation of incidents by Leidos
- some infrastructure maintenance including changing of cables on the Sydney SAN by HPE.

Despite these actions, alerts continued to be reported that indicated these actions did not resolve the potential SAN stability risk.

We 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.

Other design[4] and build decisions that contributed to the impact (both size and duration) of the incident, included:

- The SAN was neither designed nor built to cater for greater than single drive failure or single cage failure. This established a risk to our business due to the large number of business systems that depended on the SAN for normal operation.
- The SAN build included 'daisy-chain'[5] cage configuration which exacerbated the risk of errors spreading across cages as occurred during the incident. Although a viable design option at the time of SAN implementation, no evidence has been presented of subsequent options being explored by HPE to mitigate this risk.

1 Following the recent merger of HPE's services arm with Computer Sciences Corporation in April 2017, these services are now provided to us by DXC Technology

2 the 3Par 20850 Storage Area Network (SAN)

3 A 'turnkey' arrangement is one where a contractor completes a project, then hands it over in fully operational form to the client, who needs to do nothing but 'turn a key' to set it in motion

4 No evidence was presented to indicate that sufficient detail on design and/or implementation choices related to technical resilience and recovery capacity had been presented by HPE to the relevant ATO governance forums to allow them to fully appreciate, communicate and mitigate the resultant business risk. Nor was there evidence of formal analysis of business risks associated with the characteristics with the technical solution being carried out, even though ATO design governance forums accepted the design proposed by HPE.

5 Daisy-chain refers to the interconnection of technical components in a series (for example, one after the other)

- The design and build of the SAN had a relative focus on performance as part of the balance to be struck between performance, stability, resilience and cost. The design features included the overall configuration and placement of control, management and monitoring systems. An example of this is the 3PAR SAN's monitoring facility to provide automatic alerts to IT engineers not being engaged, restricting the amount of operational feedback available to HPE, Leidos and the ATO. The focus of the design and build resulted in resilience levels insufficient to cater for the size of this particular failure and led to an extended recovery as tools required to restore ATO services were stored, hence dependent, on the failed SAN.
- The firmware supporting impacted disk drives in the 3PAR SAN prevented those drives from re-booting, which impacted our ability to recover data from the affected drives.
- Issues with the stressed fibre optic cables, which we believe to be a major contributor to the incident.
- Recovery procedures for applications in the event of a complete SAN outage had not been defined or tested by HPE.

The initial outage

This section provides a detailed account of the technology and service failures that led to the outage of ATO systems over 11–12 December 2016.

The initial SAN component failure occurred late on 11 December 2016 on the 3PAR SAN located in Sydney when errors were identified on two data paths[6] leading to multiple drives across two drive cages changing state from their normal operations. Data paths include fibre optic cabling and the ports on the 3PAR SAN, and are critical to the movement of data on to and off the storage device.

In response to these data path errors, the 3PAR SAN went through a series of steps designed to automatically self-remediate. These steps included the affected drives trying to relocate data, switching between a normal and degraded state and the 3PAR SAN attempting an 'auto hard reset' in order to restart the solid state disk drives on which data is stored.

None of these automated steps were successful in returning the affected drives back to normal operations.

In response to the drives' change in state, the data volumes, which are used by applications to access storage, recognised that not enough drives were available to maintain data integrity.

This condition caused the drives to enter a preserved state. This represented the official start of the outage, occurring at 12.40am on 12 December 2016.

This particular SAN configuration leverages a feature known as wide-striping which is designed to significantly improve performance by reading and writing blocks of data to and from multiple drives at the same time, preventing single-drive performance bottlenecks. When several physical disk drives were impacted by a drive firmware issue which prevented those drives from re-booting, the result was that a small number of drives temporarily and in some cases permanently prevented access to a significant amount of application data. This also had the effect of extending the duration and complexity of the recovery effort.

We have been advised that this particular combination of events has not been previously experienced in relation to HPE 3PAR SANs.

In identifying the errors occurring with the 3PAR SAN, HPE staff commenced standard operating procedure, executing remedial activity in an attempt to restore service to the ATO.

HPE engineers continued to attempt to address these SAN issues throughout the early morning of 12 December 2016, including action at 4.50am and 6.00am. Between 6.00am and 7.00am the scale of the outage was identified as a Priority 1 (highest alert) incident, with a joint command centre established to address remediation (involving the ATO, HPE and Leidos). This was despite the conditions for Priority 1 incident being established at 3.35am. ATO business continuity procedures were invoked to address the IT crisis and to inform stakeholders.

Consequently this outage caused a general failure of most ATO IT systems, including our website **ato.gov.au** and the availability of our top six applications:

1. ATO online services
   - allows individuals to lodge tax returns using myTax
2. Portals (Tax Agent, BAS Agent and Business)
   - allows business to pay amounts and lodge activity statements, and allows agents to lodge and pay on behalf of their clients
3. The Australian Business Register (ABR)
4. The ATO's Standard Business Reporting (SBR) services and AUSkey services
   - critical for the business of the superannuation industry and software developers

6 SAS (serial attached SCSI) data paths. Includes interface cards, cabling and the ports on the storage drives themselves. SAS is a point-to-point serial protocol that moves data to and from computer storage devices. In this case, it supports data transport within the SAN itself (as distinct from between the hosts and the SAN).

5 Siebel (ATO's core case management system)
   – records our interactions with clients
6 The ATO's outbound correspondence systems
   – allow us to initiate communication with taxpayers.

The second outage

Following the first outage, the 3PAR SAN was under heightened and continued monitoring to ensure that any issues with the SAN were identified as soon as possible whilst remedial action was undertaken. HPE brought in local and international experts to work with the ATO in restoration, in identifying causes, and in trying to improve the resilience of our Sydney 3PAR SAN. Throughout the course of the investigation, fibre optic cabling issues were identified which we consider to be a key causal factor to the initial outage. As a result, increased monitoring and replacement of some cables took place to mitigate the risk of further outages.

Unfortunately, during one replacement exercise, we were informed that data cards attached to the SAN were dislodged. This caused the 3PAR SAN to act in a similar way to that noted during the December outage. This included unsuccessful steps to automatically remediate, followed by a system shut-down to preserve data integrity. HPE communicated this Priority 1 incident to us immediately.

Since the second outage, we have been advised by HPE that the successful replacement of affected cabling has coincided with data path alerts completely stopping.

ATO's response to and recovery from these outages

The first outage was briefed to the ATO Executive by 8.00am on 12 December 2016. This caused the formation of our highest level Crisis Management Team (CMT) to direct recovery. CMT took carriage of:

- understanding the causes of the issues
- supporting service providers and ATO IT specialists in addressing resumption of services
- coordinating across all stakeholders in the tax and superannuation systems, including the community, government, clients, professionals, ATO staff, industry groups and partner agencies
- overseeing business resumption planning.

ATO business recovery process generally worked very well, with high levels of collaboration and support across the organisation.

Stakeholder communication was challenged by the unavailability of our website **ato.gov.au**. However, a variety of channels including personal networks and social media were deployed to keep people informed.

We have standard practices to manage our responses when there are events that impact stakeholders. In line with those practices, an overarching communication strategy was developed and implemented. A combination of channels was used to deliver information and advice internally and externally. In particular:

- social media channels were used to provide immediate information and updates to the broader community, and as a platform to respond to general enquiries
- media releases, Commissioner's statements and interviews were used to provide more detailed updates and respond to specific requests for information
- regular, targeted alerts were issued to tax practitioners, software developers and super funds to support their specific circumstances.

Feedback from stakeholders about ATO communications was very positive.

Snapshot of ATO engagement with community and stakeholders in December 2016

The ATO provided:

- 15 publicly available ATO systems updates, which were posted to the 'Let's Talk' website and the Media Centre within **ato.gov.au**, including:
  - the initial media statement from acting CIO on 13 December
  - the public statement from the Commissioner of Taxation on 16 December.
- 98 ATO social media messages via Facebook, Twitter and LinkedIn (which supported and reinforced the above public updates).
- 27 tailored messages (via bulk e-mails, SMS messages and newsletters) to the tax professional community.
- 23 tailored messages (via webpage updates, bulk e-mails, newsletters and articles) to the software developer community.
- 26 tailored alerts to APRA-regulated superannuation funds.

Initial advice suggested that ATO systems would be restored for business on 13 December. However, this expectation was not met for a variety of factors, including the difficulty in accessing remedial tools which HPE had stored on the 3PAR SAN that had failed. Later on 13 December some key systems became available, although the services which are supported by these systems were not operating with full functionality:

- **ato.gov.au**
- payment systems
- ATO case management system (Siebel).

By 15 December most priority programs or applications had been restored, with most systems functional by 20–21 December 2016. This involved high levels of collaboration between IT experts in the ATO, contract partners including HPE, and local and international experts.

Technicians from the ATO and HPE worked around the clock during this period, including significant activity over the Christmas break, in a concerted effort to bring systems back online and restore our services.

Following the outage on 2 February 2017, the range of systems and services impacted was similar to those impacted in the 12 December incident. The primary exception being our website **ato.gov.au** which had greater availability on this occasion due to it being subsequently moved to a cloud based environment. A similar approach was adopted to quickly invoke the ATO's Crisis Management Team to lead recovery and coordinate communications. Given the experience of December 2016, our responses were more timely with systems available on 6 February 2017, with clearer stakeholder communications.

Snapshot of ATO engagement with community and stakeholders in February 2017

- 10 publicly available ATO systems updates, which were posted to the 'Let's Talk' website and the Media Centre within **ato.gov.au**, including: – The media statement from the Commissioner of Taxation on 8 February confirming our commitment to deliver Tax Time 2017.
  - supported and reinforced by 23 ATO social media messages via Facebook, Twitter and LinkedIn.
- Eight tailored messages (via bulk e-mails, SMS messages and newsletters) to the tax professional community, as well as phone briefings and a letter to the tax professional community.
- 15 tailored messages (via webpage updates, bulk e-mails, newsletters and articles) to the software developer community and phone briefings.
- Eight tailored alerts to APRA-regulated superannuation funds, phone briefings and a letter to superannuation industry.
- Phone briefings with stakeholders were chaired at a Deputy Commissioner level and provided a means for these stakeholders to express their concerns.

Post incident review activities

On 16 December 2016 the ATO announced there would be a comprehensive review into the cause of the incident, and the effectiveness of our response. On 20 December PwC were appointed to conduct the independent review into the cause of the outage.

As a part of activities to ensure full service restoration and the stability of our data storage systems, it was agreed between ATO and HPE that the 3PAR SAN that failed would be fully replaced.

In parallel to the PwC review, HPE advised they would be undertaking a root cause review of the hardware that failed. The examination by HPE is ongoing, with further investigation required to answer specific technical questions, including:

- The impact of environmental factors at the Sydney site such as the state of the active fibre optical cabling.
- The cause of the noted increase in related errors, and what action HPE took to address these issues.
- The impact of HPE support actions initiated on 11 and 12 December 2016.
- The effectiveness of 3PAR SAN firmware designed to support disk drives.
- Other causal factors leading to the failure of the 3PAR SAN.

This root cause examination cannot be completed until the SAN is physically removed and taken back for forensic testing. This process may not be completed until late 2017.

An internal ATO review was also initiated to review the crisis management response and to seek feedback from clients and stakeholders about their experiences.

Understanding the impacts and opportunities for improvement

Stakeholder impact

The systems outage disrupted ATO programs for the collection and refund of revenues, delivery of services, collection of intelligence and data to test and support government policy. More specifically the outage had material impacts on some of our key stakeholders:

- Superannuation industry – the unavailability of certain services and platforms prevented APRA-regulated funds from managing member's accounts including making contributions to those accounts.
- Tax practitioners/intermediaries – the unavailability of the portals preventing them from access their client's accounts and lodging, paying or requesting refunds on behalf of their clients.
- Software developers–- the unavailability of certain services inhibited their capacity to deliver new or updated products.

Notwithstanding these impacts, these two outages had no material impact on our program of collecting revenue. Further, all tax refunds scheduled to be delivered to clients prior to Christmas 2016 were processed by that time.

Rather than the impact on the ATO's goals, we were more focussed on understanding the impact of the systems outage on our clients and stakeholders. We conducted a range of meetings with clients, including tax practitioners, professional/industry associations, representatives from software producers and the superannuation funds. In addition, we received numerous written submissions. The following section summarises this feedback from stakeholders, enabling us to test and inform future approaches to our business including IT service delivery and business continuity.

Communications and engagement

Stakeholders were generally appreciative of regular ATO updates on the readiness of IT services. This included our acceptance of responsibility, and apology to those who had been disadvantaged. The use of social media provided a flexible channel to reach a large audience, especially during the initial outage when our website was unavailable.

Particular stakeholder groups were contacted by their ATO lead relationship managers to provide detailed updates and to answer questions. For example, key members of the superannuation industry appreciated a regular teleconference update during the second outage in February 2017.

Stakeholders sought information so they could inform their clients. Some feedback suggested that some of our information about the outage could be clearer, for example:

- Suggesting services would be restored by a particular time and this timeline was not met. Clearer messages allow stakeholders to better manage their own businesses and timeframes (for example, tax practitioners could better roster their staff to complete lodgements).
- The use of generic descriptions such as 'ATO online functions' did not clearly explain what systems or services were impacted or were scheduled to be restored.
- Inconsistent messaging coming from the wide range of communications channels used by the ATO. There is a challenge to ensure messaging across multiple channels is consistent. This has a particular effect on our partners (tax professionals and software developers) if they are receiving different messages from each other and their clients.
- When we advised the community ATO systems were restored, we needed to caveat that some services were slow, and/or would not be instantly available due to service whitelisting[7]. This clarity would have assisted tax professionals in better managing their clients' expectations.

Whole of system responses

Stakeholders recognised that IT failures were a regrettable reality in the 21st century. However they expected that our disaster recovery processes would have a more integrated approach across the entire tax and superannuation systems. The ATO's IT system is not the only technology system in the broader tax environment, and they are all interconnected and interdependent. We need to recognise this interconnectedness and that delivering outcomes is not dependent solely on ATO technology.

There was broad agreement that while it works well, our business continuity planning and information needs to span the entirety of services regardless of who owns each piece of technology. The ATO should examine the extent of which they can share its business continuity protocols with key stakeholders to improve their processes. Links could be built between these processes to provide more service strength and resilience across the entire tax and superannuation system.

Ownership of technology platforms

The ATO's IT system is one part of an interconnected IT system across the entire tax and superannuation systems. It is integral we understand the ATO's role and the role of others in this broad ecosystem. With an increasing number of third parties operating in the ecosystem (such as software developers) there is suggestion this gives rise to a need for shared operating risks that need to be managed across the collective.

There were also suggestions about the broader roles and responsibilities non-government entities should have in the design and management of technology infrastructure that delivers functionality relied on by both government agencies and non-government entities.

7 Whitelisting is the practice of specifying a list of approved and trusted software applications that are permitted to be present and active on a computer system. It is a more practical and secure method of securing a system than prescribing a list of untrusted software applications that are to be prevented from running on a computer system (a blacklist).

Forward planning impacts

Stakeholders explained that relatively short systems outages can have longer term impacts on their future production plans. For example, software developers rely on constant interaction with ATO IT platforms (beta platforms for testing and development of their software products) to ensure their products service their own clients. Short ATO systems outages can have serious impacts on production schedules and therefore managing expectations of their own clients.

Priority restoration of services

Stakeholders also noted that the ATO could be more client-focussed in prioritising which systems are reactivated after an outage. For example, stakeholders sought earlier access to systems that would support their businesses in the future, such as earlier access to e-commerce platforms for tax practitioners before access to the Tax Agent Portal, to enable them to continue their business operations. In addition, we recognised the need for clearer communications by reinstating our website **ato.gov.au** to the cloud.

We also had regard to our financial obligations to government, including re-activating our payment system, and implementing workarounds to accommodate important policy announcements. For example, while employers had a deadline of 31 December 2016 to register into the new system to withhold tax from temporary resident working holiday makers, we effectively extended until 31 January 2017, by administrative concession.

Compensation for disadvantage

Whilst some stakeholders raised the issue of compensation in their submissions or in meeting with us, to date, we have received only a handful of claims. Throughout the period and since that time deferrals for lodgement and payment, discretions and waivers under the tax and superannuation laws have been applied both individually and across the affected population to support those disadvantaged by the systems outage. For example, APRA and the ATO coordinated to allow superannuation funds to lodge later outside normal timeframes without penalty. This support is also continuing with agents as they work to clear their backlogs.

Some feedback included that the CDDA scheme was inflexible to deal with a major outage that impacted many stakeholders. We believe that the CDDA scheme provides a fair system for making payments to those who can evidence disadvantage and will consider any claims received on their merits. The scheme balances the need to make compensation payments in appropriate circumstances with the need to carefully manage the expenditure of public moneys.

Service standards

Some stakeholders raised the option of the ATO providing IT systems with more precise service standards. Improved or tighter service standards are increasingly common in digital commercial transactions. Against this option was the recognition that our systems are generally provided to stakeholders free of charge and therefore in distinction to commercial IT provision.

Recommended improvements

The ATO is committed to making the following recommended improvements. Actions in response to the majority of the recommendations are already underway, with the current status for each recommendation listed below. Additional detail is included in the final section: *Future Directions*.

Theme 1 – Principles informing the ATO's IT design

Rec 1.1 – The design and implementation of the ATO's 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 the ATO's future IT sourcing program.

Current status *– We continue to survey the current design of our IT infrastructure, to identify how best to balance the performance of our IT systems with an appropriate level of stability and resilience, all within the consideration of efficiently spending public funds.*

Rec 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.

Current status *– We are committed to supporting the government's IT agenda, while we continue to examine how best to align the agency's corporate objectives with the prioritisation of our IT investment strategies. Every year, the ATO's priority focus is for a successful implementation of Tax Time, and following a successful Tax Time 2016 and improved IT infrastructure we are confident we will deliver an equally successful Tax Time 2017.*

Theme 2 – Correcting the identified faults

Rec 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.

Current status *– The ATO has developed a new storage strategy to enhance IT stability and resilience. This involves rebuilding our primary and back up storage systems with the newest technology from the HPE product portfolio working in conjunction with our 3PAR SAN technology. All production system workloads are now utilising the enhanced storage system. Once data transfer activities are completed, the existing 3PAR SAN will be replaced by a new 3PAR and the current 3PAR SAN decommissioned by late July 2017 for forensic analysis.*

Rec 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.

Current status *– Completed – The current 3PAR SAN at Sydney, containing the disk drives which experienced the errors has been replaced by new 3PAR SAN equipment including new disk drives, with the existing 3PAR SAN to be decommissioned by late July. Further, HPE and its sub-contractors have prepared a software update for the ATO to prevent further incidents.*

Rec 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. The ATO should also re-architect these control systems to provide 'always on' capability.

Current status *– Completed – This has been addressed as part of the new overarching storage infrastructure design and strategy.*

Rec 2.4 – Review and risk assess ATO infrastructure to improve resilience and mitigate the impact of a complete data storage failure whist 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.

Current status *– the newly built data storage system which includes enhanced technology consists of a four part storage configuration and increased data replication, which provides the appropriate back-up and fail-over abilities as well as enabled monitoring and resilience features.*

Theme 3 – Enhancing ATO capability to support infrastructure design and IT governance

Rec 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.

Current status *– planning in progress*

Rec 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.

Current status *– planning in progress*

Rec 3.3 – Improve the analytics function of the ATO's centralised logging capability while still applying the appropriate balancing 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.

Current status *– planning in progress*

Theme 4 – Incident responses for the ATO and the wider tax system

Rec 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.

Current status *– The ATO are continuing to work on improving existing business continuity management processes. As part of the design of the ATO's IT infrastructure, we will commit to examine the feasibility and in particular cost effectiveness, to ensure the most appropriate level of dedicated run function is established.*

Rec 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.

Current status *– While the incident highlighted how well the natural order of the ATO's business continuity management functioned, it highlighted the need for the underlying process to be better documented for those who may not be as experienced as the current ATO staff involved in this area. We are currently working on updating and improving existing business continuity management process documentation.*

Rec 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.

Current status *– planning in progress*

Theme 5 – Managing communication and business resumption with stakeholders

Rec 5.1 - In the event of an unscheduled, high impact, disruption to ATO services, to support the transparency and regularity of our communications, we needs to improve key stakeholder communications, ensuring they are tailored to each particular stakeholder's experience.

Current status *– While the incident highlighted the effectiveness of the ATO's public communications, including the timeliness, amount and use of multiple channels, it did highlight some areas for improvement. The ATO is currently working to make these improvements, in particular developing ways to tailor the content of the communications based on describing what is currently happening and / or being done, and how that will directly affect different clients.*

Rec 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.

Current status *– While the ATO has a long standing commitment to applying waivers when stakeholders are impacted by no fault of their own, the ATO is working on improving how we clearly communicate how and when general waivers will apply in particular circumstances.*

Future directions

In an increasingly digital environment, eliminating all risk of IT failure is impossible. The ATO is committed to understanding the cause of failures when they occur, and to apply these insights to enhance the services we provide to the community. We want to be open about these insights because they also may be valuable to other stakeholders. This section of our report describes how our storage system has been rebuilt to provide world class performance and resilience. We also describe how we are applying the lessons from these incidents into our future IT plans (including new technology and new partners) to enhance services for our clients.

In developing IT plans, we are very conscious of community expectations to deliver services:

- via effective and easy to use digital channels, with high levels of performance
- using stable systems that are generally available (apart from pre-planned maintenance outages)
- with high resilience, which refers to the timely resumption of services following a critical incident or an unexpected disruption
- efficiently, recognising our obligation to be diligent when spending public funds.

In balancing these various considerations, we had previously made choices about the 3PAR SAN which focused on performance and cost efficiency over resilience. This meant we had manual fail-over systems for critical parts of our infrastructure. We now appreciate that those timeframes associated with resuming our services do not meet community standards. That is why we are making changes to our IT strategies and infrastructure.

The rebuild of our storage network is illustrative of our new approach. First, we thoroughly reviewed the causes and consequences of our systems outage via a post-incident internal review. We required HPE to commence their root cause review, and brought in independent experts to support the technical analysis of complex IT issues. The value of this investigation was proven when HPE ordered a replacement for the Sydney 3PAR SAN with a new model SAN.

In addition, HPE identified a software fault that impaired SAN disk performance in our SAN. HPE and its sub-contractors prepared a software update or patch for the ATO and for all their other clients in similar circumstances to prevent further incidents.

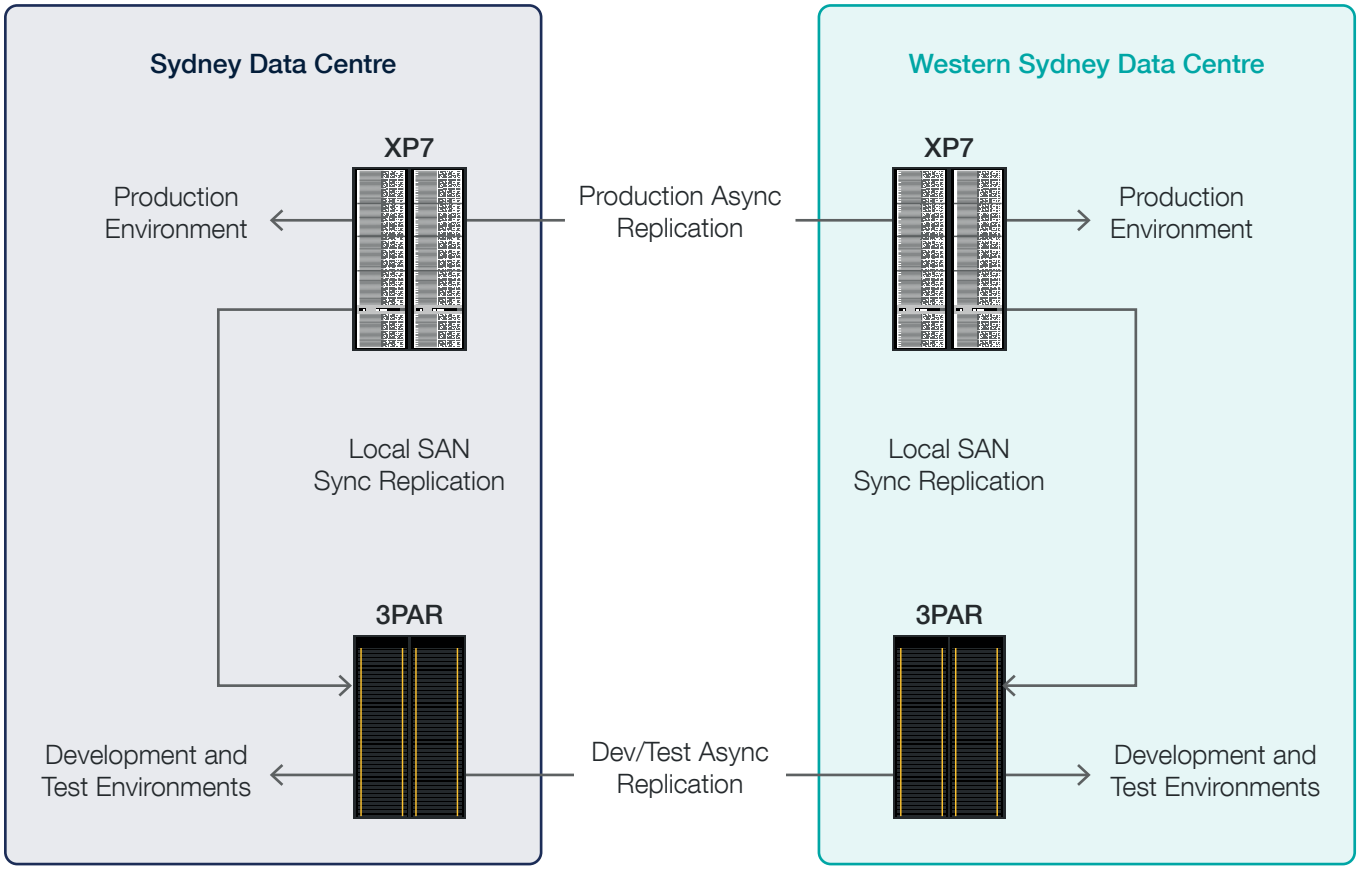
Second, with our review and with expert assistance, we developed a new storage strategy to enhance IT stability and resilience. This involves rebuilding our primary and back up storage systems with a HPE multi-tiered SAN solution working in conjunction with our 3PAR SAN technology in both our Sydney and Western Sydney sites. This four-part storage configuration and increased data replication, provides the community with world class facilities and a very high degree of resilience.

Figure 1 was designed by the CTO Group and provides an overview of how these SANs operate together.

Whilst it was regrettable to require a scheduled outage of our systems over the Easter 2017 long weekend, this storage reconfiguration has now been successfully implemented, and gives us a high degree of confidence that we can support our clients in Tax Time 2017.

Insights from our IT experiences will also inform our future IT acquisitions. As contracts come up for renewal, we need to balance service, stability, resilience and cost. Our IT program continues to prioritise government policy reforms and ATO corporate priorities, with a primary focus on another successful Tax Time for 2017. Future sourcing of IT is also influenced by whole-of-government initiatives, including closer collaboration with the Digital Transformation Agency. These initiatives will support and enhance our capability as we harness new technologies to provide better services to all Australians.

Figure 1


Sydney Data Centre
XP7
Production Environment
Production Async Replication
Local SAN Sync Replication
3PAR
Development and Test Environments
Dev/Test Async Replication
Western Sydney Data Centre
XP7
Production Environment
Local SAN Sync Replication
3PAR
Development and Test Environments

Appendices

Appendix A – Timeline of events

Pre-incident

1 July 2012

- Termination of contract originally signed with Electronic Data Systems (EDS), after the company was acquired by Hewlett Packard Enterprises (HPE) and a subsequent new five-year contract was signed with HPE. Commencement of a stabilisation year arrangement with HPE to assure the transition to the new Centralised Computing (CC) service arrangements.

1 July 2013

- Five-year contract term with HPE for CC services commenced.

Early 2015

- Process commenced to consider refresh of Storage Area Network (SAN) infrastructure at the Sydney data centre.
- In early 2015, a sourcing, design and implementation process commenced in relation to the ATO's Storage Area Network (SAN) solution.
- As part of the services it provided under the CC contract, HPE recommended the installation of a 3PAR SAN to replace the existing EMC Corporation SAN on the basis that the 3PAR solution:
  - created a more flexible storage environment that would better optimise costs
  - provided grater performance over the existing solution
  - was supported by HPE operating procedures and technical expertise.
- This recommendation was considered and endorsed by technical and governance bodies within the ATO's Enterprise Solutions & Technology (EST) Group.

November 2015

- Completion of installation of the new HPE 3PAR SAN at the Sydney data centre.

November 2015 – May 2016 – Build and Operation of the SAN

- Operation and maintenance of the SAN was the responsibility of HPE. The ATO had no direct access to the SAN(s) or its parent data-centre(s) in the normal course of operations.
- Design and build decisions made by HPE for the SAN (including array configuration, placement of control / management / monitoring systems[8]) resulted in resilience levels insufficient to cater for the scale and scope of the technical failure, and also led to an extended recovery duration.
- The SAN design/build implemented by HPE did not include available, automated technical resilience and data/system recovery features (such as 3PAR Recovery Manager and Peer Persistence).
- Recovery procedures for applications in the event of a complete SAN outage were not defined or tested by HPE.
- Processes for data reconciliation in the event of an outage of this nature had not been documented and verified.
- Comprehensive data volume-to-server-to-application mapping information had not been maintained (and therefore were not made available to parties executing the response/ recovery process).
- Sufficient detail on design and/or implementation choices related to technical resilience and recovery capacity was not presented by HPE to the relevant ATO governance forum(s) to allow them to fully appreciate, communicate and mitigate the resultant business risk.
- The ATO's associated governance was not robust and relied heavily on HPE recommendations.
- Full automated fail-over for the entire suite of applications and services in the event of a complete Sydney array failure had not been considered to be cost-effective.

May 2016 – November 2016 – Alerts to potential SAN failures

- Since May 2016, at least 159 alerts were recorded in SAN device monitoring and management logs (SNMP logs).
- At least 77 of these alerts, related to components that were observed to later fail on 11–12 December 2016, were logged in our incident resolution tool managed by Leidos.
- Some actions had been initiated by HPE in response to / related to these indicators, including:
  - collation of incidents by HPE
  - some incidents were escalated to the labs in the US for further investigation which highlighted the potential consequences but not likelihood of a major incident
  - some infrastructure maintenance / remediation, including changing of cables on the SAN by HPE.

However errors continued to be reported that indicated these actions did not resolve the potential SAN stability risk.

- In early November 2016, the ATO experienced a two to three hour systems outage that impacted the availability client facing services.

8 Control / management / monitoring systems were deployed with significant dependency on the impacted SAN. These systems also suffered an outage extending the duration of recovery activities post-incident.

The incident

11.27pm on 11 December 2016

- The initial SAN component failure occurred on the primary Sydney SAN. Excessive errors were observed on two data paths[9] leading to a changed state (changed from normal operations) on multiple drives across two drive cages (cages 12 and 13).
- In response to these errors, the SAN then went through a series of automated steps to self-remediate, including that:
  - the drives (in cages 12 and 13) tried to relocate data
  - the drives toggled between normal and degraded state
  - the SAN attempted 'auto hard resets'
- None of these actions were successful in returning the affected drives to normal operations.
- The primary Sydney SAN was attended to by a HPE engineer.

12.40am on 12 December 2016 (Day 1)

- Corrective actions were undertaken by a HPE IT engineer, 12 solid state drives were restarted in an erroneous state.
- In response to the drives' change in state, the data volumes (which are what applications use to access storage) recognised that not enough drives were available to maintain data integrity (n-1 parity).
- This condition triggered them to enter a 'preserved' state. This change of state represented the official start of the outage.

12.40am–3.35am on 12 December 2016 (Day 1)

- A significant number of volumes were in this 'preserved' state (455 out of 3,063 volumes). The incident had now met ATO specified conditions for categorisation as 'Priority 1' but HPE did not make this categorisation at this time.
- This particular SAN configuration leverages a feature known as wide-striping which is designed to significantly improve performance by reading and writing blocks of data to and from multiple drives at the same time, preventing single-drive performance bottlenecks. When several physical disk drives were inpacted by a drive firmware issue which prevented those drives from re-booting, the result was that a small number of drives temporarily and in some cases permanently prevented access to a significant amount of application data, with that impacted data subsequently and successfully restored from both tape and disk-based backup systems.

4.50am on 12 December 2016 (Day 1)

- HPE support actions initiated (specifically, drives in cages 12 and 13 were power cycled via remote command line).

6.00am–7.00am on 12 December (Day 1)

- A senior HPE IT engineer identified messages relating to corrupted solid state drives, and the scale of the impact on ATO services was first identified. HPE commenced diagnosis of the issue.
- The incident was escalated to a Priority 1 (highest alert).
- A command centre constituted by the ATO, HPE and the Enterprise Service Management Centre (a service provided to the ATO by Leidos) was established.

10.15am on 12 December 2016

- The ATO's primary midrange services were identified as being unavailable including the ATO website **ato.gov.au**, and our 'top six applications':

1 ATO online services
  – allows individuals to lodge tax returns using myTax

2 Portals (Tax Agent, BAS Agent and Business)
  – allows business to pay amounts and lodge activity statements, and allows agents to lodge and pay on behalf of their clients

3 The Australian Business Register (ABR)

4 The ATO's Standard Business Reporting (SBR) services and AUSkey services
  – critical for the business of the superannuation industry and software developers

5 Siebel (ATO's core case management system)
  – records our interactions with clients

6 The ATO's outbound correspondence systems
  – allow us to initiate communication with taxpayers.

9 SAS (serial attached SCSI) data paths. Includes interface cards, cabling and the ports on the storage drives themselves. SAS is a point-to-point serial protocol that moves data to and from computer storage devices. In this case, it supports data transport within the SAN itself (as distinct from between the hosts and the SAN).

ATO's response and recovery to the incident

8.12am on 12 December 2016 (Day 1)

- Senior management were notified of widespread server issues. The Incident Management Team was tasked with investigating.

8.40am–8.50am on 12 December 2016 (Day 1)

- A severity 1 incident was raised, with management notified and crisis management protocols initiated.
- On the basis of the initial assessment, Crisis Management Team Level 2 (CMT2) was triggered to coordinate all ongoing response activities. Communications were issued to stakeholders via available channels. CMT2 coordinated, controlled and managed business level activities throughout the period of the incident.
- The ATO's acting CIO was advised of the severity 1 incident, the general scope of the impact and that diagnosis of the problem was underway.
- ATO business areas were engaged with an agreement to convene every two hours while the incident was investigated.

9.21am–9.30am on 12 December 2016 (Day 1)

- Communication to all internal staff issued.
- External stakeholders advised of the issues via social media.
- Ongoing internal and external communications were issued throughout the day as the nature and extent of the incident became apparent.

2.30pm on 12 December 2016 (Day 1)

- Business continuity management arrangements had commenced and first CMT2 meeting held.

6.15pm–11.00pm on 12 December 2016 (Day 1)

- The ATO's acting CIO advised that a significant and complex data recovery process from back-ups was required to restore service.
- Following the documented business continuity processes, the organisation issued advice via relevant channels to areas most affected to activate appropriate plans including:
  - arrangements for staff to ensure focus on productive activities. This included assignment of alternative duties to impacted staff as necessary
  - provision of updates on the IT restoration progress of priority systems
  - coordinated communication approach (internal/external)
  - stakeholder management activities, including partner agencies.
- Strategies to manage agreed priorities were established, and a critical analysis CMT2 meeting was scheduled for 9.00pm.
- Initial information from the ATO's Enterprise Solutions and Technology (EST) group indicated that systems would be available for start of business on 13 December.
- The Business Continuity Management team were in early contact with the Crisis Management Team (CMT) Level 3 Leader regarding the status of the incident. Level 3 is the highest crisis management level the ATO invokes.

9.00pm–11.00pm on 12 December 2016 (Day 1)

- CMT2 reconvened with the CMT3 Leader in attendance.
- At this meeting updates made it apparent that business services were not likely to be restored by the start of business 13 December as previously advised by ATO EST group.
- CMT3 was then activated and first CMT3 meeting held.
  - From this point, due to the scale and impact on operations and stakeholders, a decision was made to focus CMT3 on ongoing strategic management issues, with CMT2 taking carriage of all operational governance activities, with combined meetings led by CMT3 held as required.

13 December 2016 (Day 2)

- With system issues persisting on the morning of 13 December, CMT focus was placed on messaging to stakeholders. A thorough approach to both internal and external communications was agreed to by the group.
- Guided by advice from ATO's EST group regarding updates on the incident, the ATO agreed that combined CMT2 and CMT3 meetings would be held every two hours through the morning on 13 December, with the ATO's Business Continuity Management (BCM) area to convene additional meetings, as required.
  - These CMT3 meetings continued to occur 2–3 times/day for the first week following the incident; and then daily until the Christmas closedown; 2–3 times/week until the end of the first week of January; and then weekly for the remainder of January.
- A number of primary midrange services began to become available, including:
  - **ato.gov.au**, which was promoted to the cloud and became available
  - payment systems came back online
  - Siebel became available with decreased functionality.

13 December – 16 December 2016 (Days 2–5)

- Services were progressively restored following the existing priority schedule with most priority services functional by 15 December 2016:
  - AUSkey services were restored (on 14 December) with decreased functionality
  - ATO portals were restored with full functionality
  - ATO online services were restored with partial functionality.
- HPE provided the ATO with updated advice in relation to the incident.

17 December (Day 6)

- Once a reasonable level of certainty was able to be achieved with respect to the availability of core systems, focus shifted to resumption strategies and associated messaging to staff and stakeholders.

18 December (Day 7)

- The ATO contacted HPE to indicate that at that point most client facing systems were only operating at a base level of capacity and there was significant work required to return systems to full capacity.
- The ATO sought greater assistance and assurances from HPE regarding the priority of the work, stability of the system and strategies to eliminate the single point of failure in the system.

20 December (Day 9)

- Standard Business Reporting (SBR) 1 and 2 services were restored with full functionality.

21 December (Day 10)

- The Australian Business Register (ABR) became available with full functionality.

22 December (Day 11)

- The Commissioner of Taxation contacted HPE and ordered HPE to supply the ATO with a new SAN to replace the affected SAN in Sydney.

23 December (Day 12)

- Critical client and staff systems were restored to minimal viable product.
- Some services (**ato.gov.au**, ATO online, ABR, portals) became briefly unavailable in the morning due to the unavailability of servers.

24 December 2016 – 2 January 2017 (Week 3)

- As priority functionality was restored, in line with incident management procedures, the frequency was reduced and daily CMT meetings continued through the ATO shutdown period, from 24 December 2016 to 2 January 2017, to oversee restoration and resumption activities.

2 January – 8 January 2017 (Week 4)

- From early January 2017, reporting of system issues reverted to business-as-usual procedures.
- A scheduled disruption to service occurred across the weekend (7–8 January) to undertake SAN restoration and stabilisation work.

10 January 2017 (Week 4)

- The build and maintenance of some SAN components (including cabling) were subject to examination by HPE following the incident.
- HPE made several observations regarding the cabling (captured in a report entitled ATO Site Findings: Engineering Review, Revision — 4.2, January 10, 2017).

11 January 2017 (Week 4)

- It was agreed that the CMT3 group would continue to meet weekly through January, while the CMT2 group would continue to meet, as required, to manage outstanding issues.

14–15 January (Week 5)

- Another scheduled disruption to service across the weekend occurred to undertake SAN restoration and stabilisation work, principally cable replacement.

Early 2 February 2017

- The system issues arising as a result of SAN faults were detected in early morning on 2 February 2017.
- The range of systems and services impacted was similar to those impacted in the December incident. The primary exception being the ATO website **ato.gov.au** which had greater availability on this occasion due to it being moved to a cloud based environment following the December incident.
- Senior ATO management were notified of the new incident early on the morning of 2 February. The Incident Management Team was tasked with investigating.

7.30am on 2 February

- CMT2 and CMT3 were notified of the new incident with a severity 1 incident raised. Crisis management protocols were initiated.
- Directly impacted ATO staff were identified and advised at the time of the severity 1 incident being raised.

10.30am on 2 February

- CMT3 convened to determine the priority action to be undertaken and agree on a coordinated approach to CMT2 and CMT3 activities.
- It was agreed that the CMT3 would meet as required – in line with updates from ATO's EST group – with CMT2 continuing to oversee operational activities and agree on specific actions required for the duration of the incident.
- Making use of existing arrangements in place from the December incident, contingency plans were initiated and updated communications were issued.

Remainder of 2 February 2017

- Ongoing internal and external communications were issued throughout the duration of the day, utilising processes and channels established for the December incident.

3 February – 5 February 2017

- CMT activities continued through to the weekend of 4–5 February.

5 February – 6 February 2017

- The majority of ATO systems became available over the evening to early morning of 5–6 February 2017.