PTS ENHANCES CLIENT'S IT DISASTER RECOVERY PLANNING AND TESTING FOR APRA CPS230

Following the migration of their Disaster Recovery (DR) Data Centre from Sydney to Melbourne, the client faced the challenge of ensuring their annual Disaster Recovery Testing would meet the new APRA CPS230 standard for Operational Resilience. With key personnel leaving the company, they turned to PTS.

REVITALISING THE DISASTER RECOVERY PROCESS

The data centre migration had brought about significant changes, including new IP subnets, firewall technology, and server names. This necessitated a thorough review and update of all existing documentation, including DR Command Centre documentation, IT infrastructure plans, and application service designs. Missing documentation was identified and created, and a recovery sequence was developed in collaboration with the infrastructure and applications teams.

OVERCOMING TESTING CHALLENGES

Initial testing revealed connectivity issues between applications and databases, primarily due to missing firewall rules and mismatches in application configurations. These were addressed, and recovery plans were revised accordingly. Additionally, a potential issue was identified with the use of virtual desktops residing in the production data centre. To mitigate this, a cloud-based virtual desktop solution (Microsoft Azure Virtual Desktop) was implemented near the DR Data Centre.

REFINING THE DISASTER RECOVERY TEST

The scope of the second DR test was narrowed to focus on the critical applications reported to APRA, and the new virtual desktop solution was utilised. The testing process involved three levels: functional testing, integration testing, and user acceptance testing. This marked the first time business testers participated, ensuring a comprehensive evaluation from a user perspective. The results were positive, with most systems performing well and any identified issues being minor.

DOCUMENTING AND ANALYSING THE RESULTS

PTS compiled a detailed Post Test Report, documenting the test process, application status, and identified issues. The report was reviewed and approved by senior stakeholders, declaring the test successful.

LESSONS LEARNED AND FUTURE IMPLICATIONS

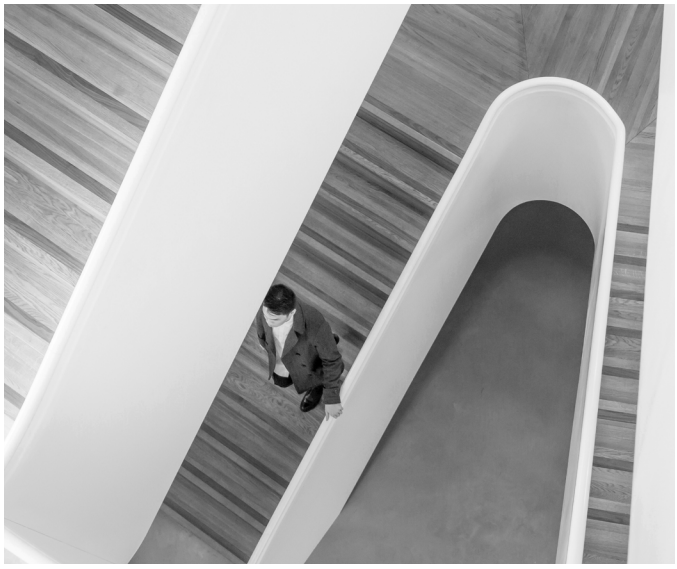
The DR testing process highlighted the importance of regular testing and alignment with production systems. It emphasised the need to integrate DR considerations into standard IT service management practices. The upcoming APRA CPS230 regulation, which mandates regular DR testing for APRA-regulated organisations, further underscored the significance of this process.

A CONFIDENT OUTLOOK

The client is now well-prepared to meet the CPS230 requirements. Lessons learned from this experience have led to improvements in change management processes, regular reviews of application DR plans, and a better understanding of the interconnectedness of DR with other IT processes. This journey has not only ensured regulatory compliance but also strengthened the client's overall disaster recovery capabilities.

CLIENT TESTIMONIAL

"Engaging PTS proved instrumental in introducing the necessary rigour to ensure our IT disaster recovery practices aligned with the stringent requirements of CPS230."



ABOUT THE NEW APRA CPS 230 STANDARD

APRA CPS 230 is a new prudential standard introduced by the Australian Prudential Regulation Authority (APRA) to bolster operational risk management across the financial sector. It aims to ensure institutions are resilient to disruptions, effectively manage operational risks, and maintain critical operations even during unforeseen events. This includes enhanced requirements for identifying and addressing weaknesses in existing controls, bolstering business continuity plans, and proactively managing risks associated with third-party service providers.

From an IT perspective, CPS 230 requires a heightened focus on the resilience and security of technology infrastructure. This involves a thorough assessment of critical systems and data, strengthening cybersecurity measures, establishing robust incident response plans, and ensuring the reliability of third-party technology providers. Additionally, it necessitates a proactive approach to identifying and mitigating IT-related risks that could disrupt critical operations, ultimately safeguarding the organisation's ability to continue serving its customers and stakeholders.