Gateway
Network
Governance
Body

2020 Superannuation Transaction Network Business Continuity Exercise Outcomes
December 2020

Background and Objectives

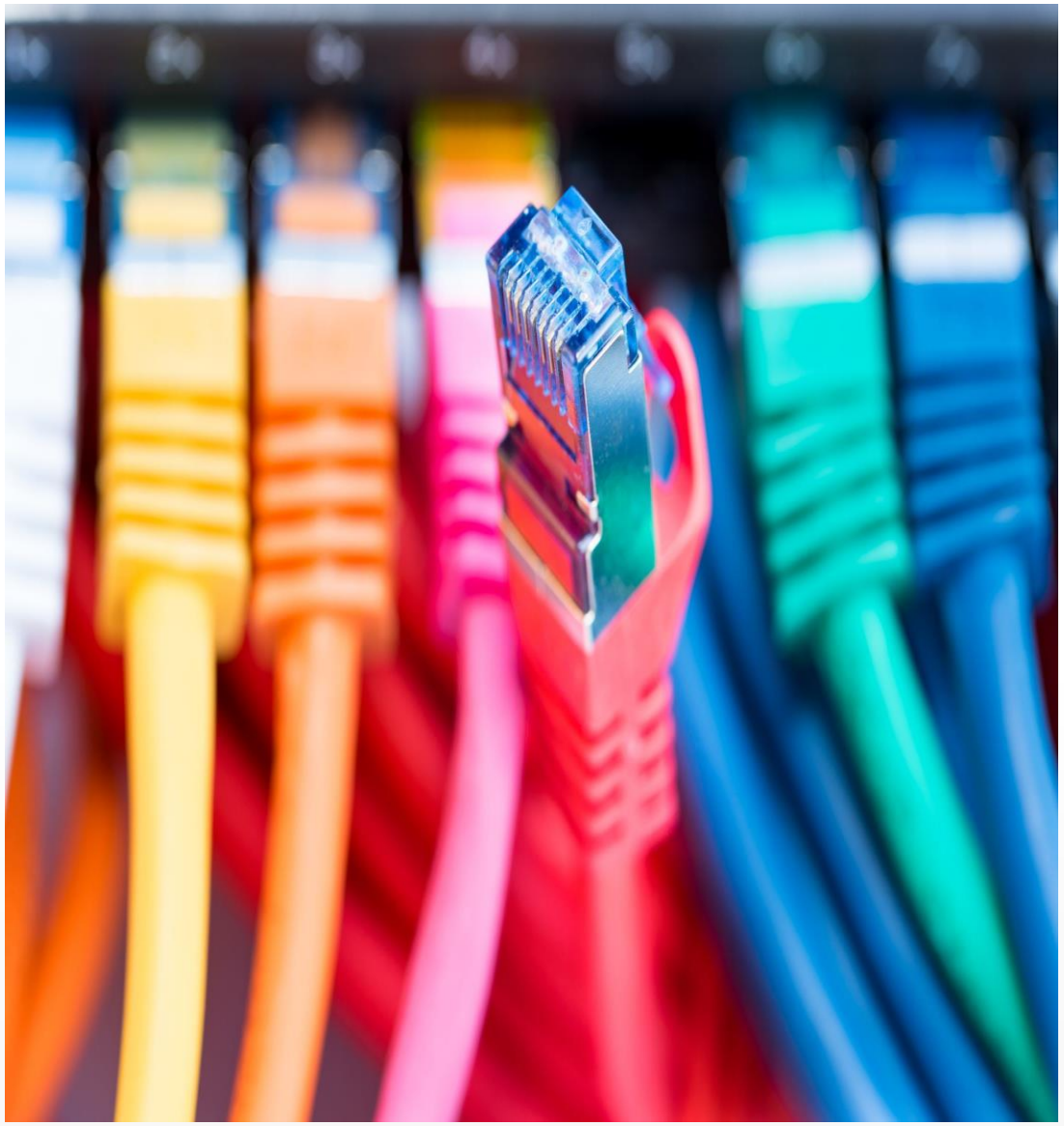
On 19 November 2020, Deloitte, on behalf of the GNGB, facilitated the **annual STN Business Continuity Plan (BCP) exercise.**

The objectives of the 2020 exercise were to:

- Conduct a high-level validation & review of the STN BCP process, with a particular focus on updated sections incorporating lessons learned from the 2019 exercise, with a view to identification of any further gaps or areas for improvement
- Test linkages between the BCP and the Cyber Incident Response Plan
- Test the ability of Gateway Operator's back-up connections to mobilise and maintain messaging continuity
- Embedding network-level business continuity management into the STN culture - a no blame, collaborative approach to resolving threats to the reliability of the network

The approach for the 2020 exercise varied from previous years exercises due to the maturity and familiarity of the plan by test participants. Key changes from previous tests included:

- A focus on familiarity and alignment of the notification and assessment steps of the process using polling to assess Gateway Operator responses, as these steps have been refined since the previous test.
- Understanding the ability for Gateway Operators to "switch" to their backup connection and the impact to other STN participants
- The exercise was conducted fully remotely, via Zoom. Gateway Operator participants were asked questions by Deloitte at regular injects with responses provided privately, or publicly if the respondent wished, to the host using the Zoom chat functionality.



Outcomes

Exercise results

The change in approach provided a positive outcome for the exercise with a number of improvements and refinements in the STN BCP identified, in particular in the notification and assessment of incidents. The STN BCP exercise resulted in in a well-coordinated response to the simulated business continuity event.

Key Observations

- All Gateway Operators and the ATO were in attendance for the exercise and there was active participation from all attendees. The use of the voting mechanism via the chat facility in Zoom assisted with participation allowing responses to be provided privately or shared with the group.
- Attendees engaged well in the discussion via videoconference and contributed openly to determine actions that should be taken in and identifying areas of refinement and improvement.
- Participants proved to be familiar with the STN BCP plan, with many having a copy at hand during the exercise, and demonstrated familiarity with the steps required and their individual roles and responsibilities.
- Assessment and prioritization steps, having been refined since the process was last tested, were a key focus and the improvements were validated. Some refinement to be addressed in definitions of impacts to provide further guidance to the response group.
- The testing of notification responses tested **all Gateway Operator responses**, not just one Gateway Operator as per previous tests. This provided evidence on how all Gateway Operators would respond should such a scenario arise and enabled discussion of the nuances of each gateway's approach.
- General feedback on the Communications Framework was that it was clear in the plan with feedback from the 2019 recommendations having being implemented.

Recommendations – the following recommendations were discussed to improve the STN BCP plan

1. It is the responsibility of Gateway Operators to advise GNGB of any updates to the Response Group Contact list.
2. Notification to GNGB of an Incident:
    a) Review wording of section 2.4 to remove any ambiguity
    b) Include a reference in the STN BCP Plan to Gateway Standards timeframes
    c) Include a statement that the Operational Notification is an “early warning” step to provide to the GNGB of a potential incident
3. Assessment of Incidents
    a) Document definition of impact of an incident to assist with the prioritisation process
    b) Review timeframes as stated in other standards and align where possible
    c) Review the plan to reflect there are variable outside the categories to prioritise that may impact assessment.
4. ATO to investigate their back-up options if the cloud service is impacted.
5. Include a definition of a Security event as opposed to a Cyber Security event (for example an internal malicious actor differs to a “cyber” event).
6. Investigate Gateway Operators ability to re-send messages on system restoration in the unlikely event of data loss.
7. Investigate the ability of Gateway Operators to throttle transactions to mitigate the risk of flooding the network once systems are restored.