KPMG

Review of ICT resilience

New Zealand Police

NEW ZEALAND POLICE

July 2019

Executive summary

Overview

This report details our findings and recommendations from the IT disaster recovery and business continuity review performed over the NZ Police's Information and Communication Technologies (ICT) function.

Due to recent events, Disaster Recovery (DR) and Business Continuity (BC) have become prevalent topics in many government departments' internal audit and assurance programmes. As NZ Police plays an important role in national emergencies and incidents, it is important to be well-prepared as an organisation so it can be resilient and support the wider public. Over the years more and more activities have become dependent upon ICT and ICT failures are becoming more critical, therefore technical resilience is also being assessed. NZ Police realise the importance of ICT resilience and have identified BC and DR as a "very high" risk in the Key ICT Risks in the ICT Operations Assurance Plan 2018/19.

Key observations and recommendations

NZ Police ICT have the benefit of experienced and capable staff which has enabled responsive management of disruptions to date. At the time of initiating this review, ownership of BC and DR was informally assigned to the Head of Service Experience, whilst DR assigned to the Head of IT Operations. Both are keen to establish and manage an effective ICT resilience programme. When concluding this review, the Head of IT Operations was made aware that DR and BC is his responsibility which is different from our initial understanding. The ICT Operations Assurance Plan 2018/19 release authority is the Chief Information Officer. The document owner is the Deputy Director Service Operations and the DR and BC activity within the plan is assigned to the DSO (Director Service Operations).

Although there is a draft BC plan and some DR documentation available, these plans are not yet comprehensive with a heavy reliance on the availability of key ICT staff to successfully activate the IT BC and DR capability. Insufficient investment and resourcing in recent years has meant ICT resilience has not been able to receive the attention needed to develop into a proactive rather than reactive programme.

There is limited understanding of NZ Police requirements for restoration of systems and services, or consequentially ICT capability to meet these expectations. As a consequence, our assessment has identified a range of opportunities to improve planning and effectiveness of the ICT resilience capability, some of which should be completed as a priority with our recommendations being to work on the following key actions:

- Formally define ownership of ICT resilience, including BC and DR. Assign clear responsibilities for performing BC and DR activities;
- Allocate budget and resources to establish and manage the ICT resilience programme;
- Develop a BC and DR framework, associated policies and processes;
- Undertake an ICT resilience risk assessment to identify key resilience related risks that need to be managed;
- Perform a Business Impact Analysis (BIA) to identify key ICT products and services, interdependencies, and recovery expectations;
- Develop recovery strategies, including target time for the recovery of ICT activities and the acceptable amount of data loss NZ Police can handle after a disruption has occurred;
- Develop and maintain realistic BC and DR plans including redundancy and failover documentation;
- Clearly identify alternative locations for ICT staff in a disruption including location details, workstations timeframe, and procedures;
- Develop an assurance plan for ongoing validation of key vendors and other third parties' resilience capability; and
- Regularly perform recovery tests and exercises.

Other considerations

With the NZ Police's planned future-state ICT projects, the ICT function is going through a major technological transformation. At this stage, it is important that availability, redundancy and resilience aspects of these upcoming or improved technologies are carefully considered. It is also important for NZ Police to understand that ICT resilience capabilities should not be designed in isolation to the operational requirements that wider NZ Police users of ICT require to maintain the safe and effective delivery of services to the public.

During the assessment we noted that although there has been a NZ Police BC policy in place for a number of years, an organisation-wide BC management framework is not available that would typically provide guidance and input to ICT resilience related requirements. Without a framework there is a high likelihood that key business processes may have ICT requirements that are not clearly understood or planned for in a disruption. A NZ Police-wide BC management framework will enable the NZ Police executive and staff to respond in a pre-planned and thought-through manner when a disruption occurs, rather than over-reliance on decisions being made under potentially stressful and time critical situations. This is particularly important if key leadership resources are unavailable due to the disruption.

Overall management response

The review has identified a number of gaps that need to be addressed such as additional resource required to implement, but has also identified that clarity is required on ownership of ICT's BCP and DR capability. We recommend that this review and the actions are given priority to ensure that Police ICT is in the best position to provide continuity to the Police organisation and the community we serve. We would like to acknowledge the assistance and support of the Risk and Assurance team enabling this review to be undertaken.