Summary - Deloitte Fraud Risk Assessment

In May 2018 MPI commissioned Deloitte to carry out a Fraud Risk Assessment. The purpose of this work was to understand the extent to which MPI is exposed to fraud and corruption risks, and how well it is positioned to manage these risks.

The risk assessment included:

- an online staff survey to capture staff perceptions of fraud;
- a gap analysis workshop with a small group of senior staff members to benchmark MPI's planning, prevention, detection and response to fraud and corruption risks; and
- a series of workshops with staff to identify and assess potential areas of fraud, and the controls to mitigate fraud and corruption risks.

In total, 433 staff completed the anonymous staff survey. The results of the survey flagged that staff had a healthy understanding of types of fraud and corruption and had a genuine willingness to raise concerns. However, the survey also indicated that staff needed greater familiarity with the available reporting mechanisms to encourage them to report fraud, and to enable them to be confident about raising these concerns.

One of Deloitte's key recommendations was the need to dedicate more resourcing to the planning and prevention of fraud, through:

- developing a Fraud Control Plan;
- enhancing existing training and awareness activities; and
- doing more regular risk assessments.

Deloitte also recommended that, irrespective of this, MPI should further develop its processes for communicating fraud and corruption risk exposures to employees, and develop targeted training for those people that have the greatest exposure to integrity related risks.

The series of workshops that Deloitte ran identified a range of potential fraud risks most of which they considered were adequately controlled. One of the categories of risk that they identified was the loss or theft of information and data by staff and external parties. Deloitte flagged some concerns about the Ministry's transparent and open approach to information particularly with respect to:

- the use of its enterprise content management system (Piritahi) as a way of sharing information across MPI;
- the degree to which information and data is stored outside this system on laptops and mobile devices;
- the way in which MPI communicates its expectations about the protection of information particularly to secondees and contract staff; and
- the inconsistent application of security classification across Sensitive and In-Confidence information.