Follow-up of the Independent review of the Ministry of Social Development's decisions relating to the IT system used to capture individual client level data

Independent Review Report

Final Report

Prepared by: Anu Nayar, Partner, Deloitte

21 March 2018

Contents

Executive summary

The Ministry of Social Development (the Ministry) funds around 2,300 Non-Government Organisations (NGOs) which are primarily community-based social service providers. As part of shifting more to a results-based investment approach to social services, the Ministry had been working with NGOs to collect some individual client-level data (ICLD) from providers.

In March 2017, the Ministry was made aware that the system used to collect ICLD from providers allowed one NGO to see the folder of another provider. This led the Ministry to commission an independent investigation into the governance and decision-making that determined the interim solution for the capture of individual client level data.

In May 2017, the initial independent review of the 'Ministry of Social Development's decisions relating to the IT system used to capture ICLD' produced four recommendations with focus on privacy, security and project management.

About this review

The objectives of this review are to follow-up on the lessons learnt and recommendations outlined in the 12 May 2017 report, to assess the progress the Ministry has made in implementing these lessons and recommendations, and to provide advice on what, if any, further actions are required to ensure these lessons continue to be embedded.

Findings

Based on our experience, the work programme to implement the lessons and associated recommendations would reasonably be expected to be completed and embedded over a 12 month period by the Ministry.

This follow up review was undertaken approximately 7 months after the 12 May 2017 report (over the December 2017 to January 2018 period). Overall, we found that the Ministry is making good progress on implementing the lessons from the May 2017 Independent Review within the period of time since the May review. Implementation of all of the lessons and associated recommendations have been commenced, and on some items significant work has been done. However, all of the initiatives still need to be embedded into the organisation and we have provided advice on areas that can be improved.

1. Learn from others	
Commenced	**Summary of Progress** The Ministry is not approving any further uses of Shared Workspaces. The Ministry has a process and a knowledge base to capture lessons learnt across projects. This process could be strengthened. **Additional Recommendations** The Ministry could benefit from making it easier for an individual or a project to learn from others, and to embed the practice of continuous learning and improvement:

	• Consider implementing a process or tool that enables staff to more easily seek knowledge and insight from multiple people within the organisation. • Update project management practices to have a consistent practice of gathering insights and implementing lessons learnt from projects as they progress. This should include at the end of each project (requiring as part of project closure), reflecting on and documenting the lessons learnt and how to do things better. On a regular basis, the EPMO should undertake analysis of the lessons learnt from projects to identify common threads, and provide the findings to governance groups across the Ministry. These common thread items can then be translated into practical actions to improve practices and capability across the organisation for improving the delivery of change initiatives within the Ministry.
2. Apply project disciplines consistently for solution deployment	
Commenced	**Summary of Progress** The Enterprise Project Management Office (EPMO) is updating project templates to trigger security and privacy considerations throughout the lifecycle of projects. **Additional Recommendations** The Ministry needs to embed the changes it is making to project disciplines, and make the following modifications: • Update the Business Case templates to require the Privacy and Information Security considerations to be within the main body of the document. • Update the project Go-Live template to specifically include Privacy and Information Security requirements, and the need for formal sign-off by the CISO and the Chief Privacy Officer. • Require within project methodologies that projects refer to the Lesson Learnt knowledge base, and formally capture and disseminate lessons learnt within the project up to governance bodies for visibility. This will enhance the Ministry's opportunities to evolve the learning culture associated with change initiatives.
3. Consider privacy early	
Progressed	**Summary of Progress** The Ministry is implementing a framework to consider not only privacy but also responsible use of information from Human Rights and Ethics perspectives. This framework called PHRaE (Privacy, Human Rights and Ethics) and has been trialled through projects and is being refined for wider roll-out. **Additional Recommendations** Continue the rollout and investment into the PHRaE framework and the operating model required to support it. This includes investing in internal

	resourcing and having knowledge transfer occur from contractor resources so that the Ministry can develop and sustain internal Privacy capability. Implement a process and the requirement to confirm that key Privacy recommendations are implemented prior to project go-live.
4. Validate information security risk mitigations	
Progressed	**Summary of Progress** The Ministry has strengthened the approach towards validating security controls with additional guidance and reporting requirements for security validation. This is currently being embedded into practice across projects and the business. **Additional Recommendations** Based on our findings, we recommend that: • As part of embedding the controls validation approach, educate projects that controls validation goes beyond just penetration testing. • Even for medium security risk projects, require evidence of a control being in operation e.g. beyond references to the design or other documentation to validate controls.

Further Thoughts

To assist the Ministry in realising greater value from its investment in Privacy, Information Security, and consistent and robust project delivery disciplines, it is important the Ministry assign central ownership for the completion of the work programme to embed the lessons across the organisation.

For an organisation with the scale and profile of the Ministry it is important to continue to evolve its learning and continuous improvement culture so that risk to the Ministry and its clients can be reduced through high performing change delivery.

In another 6 to 9 months, the Ministry should undertake an internal assessment (through the Ministry's Risk and Assurance function) on its progress on completing the work programme to implement the lessons and associated recommendations, and the extent to which those have been institutionalised across the Ministry.

Acknowledgments

We have had the full cooperation and assistance of the Ministry's staff and management team throughout this review. We are grateful for the time and assistance provided by the Ministry to help us make our findings.

Introduction and background

The Ministry of Social Development (the Ministry) delivers, or purchases from other providers, a significant part of New Zealand's social services, including a range of benefits, entitlements, and services to young people and communities. Services and assistance are provided to more than 1 million New Zealanders and 110,000 families every year.

The Ministry funds approximately 2,300 Non-Government Organisations (NGOs), which are primarily community-based social service providers. As part of shifting to a more results-based investment approach to social services, the Ministry had been working with NGO providers to collect some individual client-level data (ICLD) from providers.

As a result of collecting ICLD from providers the Ministry has an obligation to keep this data private and secure on behalf of the data providers.

In March 2017, the Ministry was made aware that the system used to collect ICLD from providers allowed one NGO to see the folder of another provider. This led the Ministry to commission an independent investigation into the governance and decision-making that determined the interim solution for the capture of individual client level data.

The 12 May 2017 independent review report of the Ministry’s decisions relating to the IT system used to capture ICLD set out four lessons learnt and associated recommendations.

The Chief Executive has commissioned this follow-up review to assess the Ministry’s progress in implementing the lessons learnt and associated recommendations, and to provide advice on what, if any, further actions are required to embed these lesson on a continuous basis.

Purpose

The purpose of this follow-up review is to determine if the Ministry has acted upon the lessons identified by the May 2017 independent review. An assessment will be made as to what recommendations have been acted upon, to what degree they have been embedded, and to provide advice to the Ministry on how to complete the embedding of these lessons across the organisation.

The terms of reference for this review are attached in Appendix A.

Approach

The review broadly comprises the following activities:

- Examination of documents developed in relation to the lessons and recommendations from the initial review
- Analysis of developed artefacts to identify if lessons have been acted upon and implemented
- Interviews with relevant personnel from the different parts of the Ministry involved in acting upon and implementing the lessons
- Discussions with key stakeholders
- Selecting three relevant projects to provide a sample view of how these lessons are being applied within change initiatives. Note: The review did not seek to comprehensively assess these projects individually

Limitations and disclaimer

This report was prepared solely in accordance with the specific terms of reference between the independent reviewer and the Ministry, and for no other purpose. Other than our responsibilities to the Ministry for this review, no member of the Review Team or their organisation undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility. We accept or assume no duty, responsibility or liability to any other party in connection with the report or this engagement, including without limitation, liability for negligence in relation to the factual findings expressed or implied in this report.

The report is based upon information provided by the Ministry and interviewees. We have considered and relied upon this information. We have assumed that the information provided was reliable, complete and not misleading, and we have no reason to believe that any material facts have been withheld. The information provided has been considered through analysis, enquiry and review for the purposes of this report. However, we do not warrant in any way that these enquiries have identified or verified all of the matters which an audit, extensive examination or due diligence investigation might disclose. The procedures we have performed do not constitute an assurance engagement in accordance with New Zealand Standards for Assurance Engagements, nor do they represent any form of audit under New Zealand Standards on Auditing, and consequently, no assurance or audit opinion is provided.

Accordingly, we do not accept any responsibility or liability for any such information being inaccurate, incomplete, unreliable or not soundly based, or for any errors in the analysis, statements or opinions provided in this report resulting directly or indirectly from any such circumstances or from any assumptions upon which this report is based proving unjustified.

Findings

The May 2017 Independent Review on the Ministry's decisions relating to the IT system used to capture individual client level data identified four lessons and associated recommendations for the Ministry. Based on our experience, the work programme to implement the lessons and associated recommendations would reasonably be expected to be completed and embedded over a 12 month period by the Ministry.

This follow up review was undertaken approximately 7 months after the 12 May 2017 report (over the December 2017 to January 2018 period). Overall, we found that the Ministry is making good progress on implementing the lessons from the May 2017 Independent Review within the period of time since the May review. Implementation of all of the lessons and associated recommendations have been commenced, and on some items significant work has been done. However, all of the initiatives still need to be embedded into the organisation and we have provided advice on areas that can be improved.

Summary

Lesson	Implementation Status	Summary of Progress
Learn from others	**Commenced**	The Ministry is not approving any further uses of Shared Workspaces. The Ministry has a process and a knowledge base to capture lessons learnt across projects. This process could be strengthened.
Apply project disciplines consistently for solution deployment	**Commenced**	The Enterprise Project Management Office (EPMO) is updating project templates to trigger security and privacy considerations throughout the lifecycle of projects.
Consider privacy early	**Progressed**	The Ministry is implementing a framework to consider not only privacy but also responsible use of information from Human Rights and Ethics perspectives. This framework called PHRaE (Privacy, Human Rights and Ethics) and has been trialled through projects and is being refined for wider roll-out.
Validate information security risk mitigations	**Progressed**	The Ministry has strengthened its process to validate security controls (mitigations) through updating of its security Certification and Accreditation process. This is being embedded into practice across projects and the business.

Detailed Findings

The detailed findings against the initial four lessons learnt and associated recommendations are set out below.

Learn from others

Status: Commenced

Following on from the 12 May 2017 Independent Review, the Ministry has decided not to approve any further use of Shared Workspaces.

The broader need for projects to learn from others is still relevant for the Ministry. While new Shared Workspaces for other purposes will not be used, there will be initiatives that can be analogous. For example, IT projects that leverage All of Government common capability or cloud services, therefore use services that are already “live” and that others are already using.

For the three projects sampled for this review, project personnel described learning from others through a combination of methods such as talking to people that have knowledge of previous similar projects, or having a sector wide steering committee. However, we found no evidence that the formal requirement in place for capturing / applying lessons learnt within change initiatives was actively being followed. Also, the Ministry could benefit from a process or tool that enables staff to more easily obtain insights from multiple people quickly, e.g. a communications tool.

The Ministry, through the EPMO, does maintain a Lessons Learnt knowledge base that is accessible from its intranet (Doogle) to support learning from others. The knowledge base provides a foundation that the Ministry can use to implement a learning and continuous improvement culture.

Currently the knowledge base contains the following information:

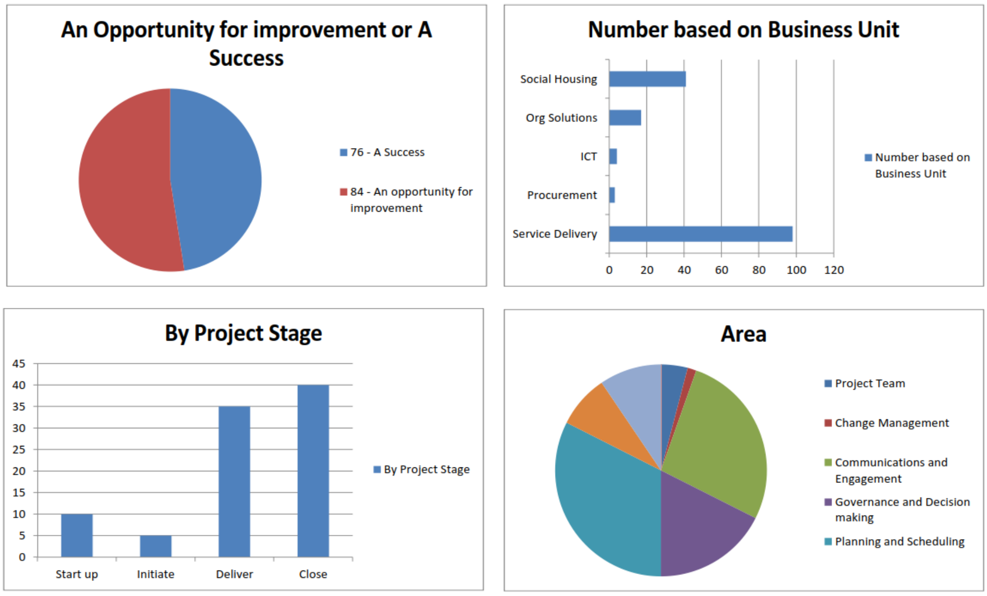

Figure 1 - Extract from the Ministry

The database has relevant lessons learnt that new projects should be leveraging. However, no updates have been made since March 2017 and based on the number of projects that the Ministry undertakes we would expect to see a higher number of entries and more current entries in the database.

High performing organisations with a culture of continuous learning and improvement, not only maintain a list of lessons learnt from projects, but also implement formal practices to enable the organisation to learn throughout their activities and embed improvements on an ongoing basis. Lessons learnt from each project are gathered, analysed, and common threads are identified and then changes are implemented. For example, the common threads of lessons learnt are reported to governance groups, and changes are made to project management or business as usual practices (where appropriate to do so). Additional training and guidance is provided to the project and operational teams to improve delivery, and to senior stakeholders to improve governance effectiveness. Over time, these efforts result in more robust project and operational delivery activities where many common and potentially significant risks are reduced.

For IT initiatives that have commonality with the use of Shared Workspace, such as the use of cloud services, one way to proactively embed lessons that others have learnt, would be to provide specific project disciplines and security and privacy guidance for cloud deployments. Currently the Ministry uses the All of Government Cloud Risk Assessment process to support cloud use. To further enhance fit for purpose project rigour and information security and privacy of cloud related service deployment, the Ministry could benefit from providing projects with specific guidance.

Recommendations:

The Ministry could benefit from making it easier for an individual or a project to learn from others and to embed the practice of continuous learning and improvement:

- Consider implementing a process or tool that enables staff to more easily seek knowledge and insight from multiple people within the organisation.
- Update project management practices to have a consistent practice of gathering insights and implementing lessons learnt from projects as they progress. This should include at the end of each project requiring (as part of project closure) reflecting on and documenting the lessons learnt and how to do things better. On a regular basis, the EPMO should undertake analysis of the lessons learnt from projects to identify common threads, and provide the findings to governance groups across the Ministry. These common thread items can then be translated into practical actions to improve practices and capability across the organisation for improving the delivery of change initiatives within the Ministry.

Apply project disciplines consistently for solution deployment

Status: Commenced

The Ministry's EPMO is currently updating project management templates. The EPMO has identified the following key documents that can be used to reinforce security and privacy thinking or requirements, which should help to promote consistency across solution deployments.

- Project Brief

  The Project Brief template is being updated to include a section that is required to be completed for privacy impact assessments, and already includes a section for considering information security. The template also includes contact information for the relevant security and privacy teams, if the project requires additional guidance or information.

- Business Case

The Business Case templates for small, medium and large projects are being updated to include a section to complete pertaining to Privacy and Security within their respective Appendices. We noted that in the body of the small and medium Business Case templates there is a section for Health, Safety and Security. The Privacy and Information Security section(s) for all business case sizes should be located in the body of the template rather than in an Appendix.

- Project Initiation Document

  The Project Initiation Document template has a section within the body of the template that is required to be completed pertaining to Privacy and Information Security.

- Project Go-Live Approval Document

  To assist the solution deployment phase, the EPMO have stated they have been working with the Chief Information Security Officer (CISO) to include the requirement that a Security Risk Assessment must have been completed within the Project Go-live template. However, at the time of the review we have not yet seen this formally included.

The three projects sampled for this review are still in progress for delivery and the solutions have not yet been deployed. Therefore, we were unable to ascertain what the specific project disciplines related to security and privacy sign-off are for these projects. The project personnel interviewed for all three projects were aware of the need to complete security and privacy activities before the solution could be deployed (i.e. before go-live) and had engagement with the CISO function for Information Security, and with the Information, Privacy, Policy and Practice (IPPP) for privacy matters.

Recommendations:

The Ministry needs to embed the changes it is making to project disciplines, and make the following modifications:

- Update the Business Case template to require the privacy and information security considerations within the main body of the document.
- Update the project Go-Live template to specifically include Privacy and Information Security requirements, and formal sign-off by the CISO and the Chief Privacy Officer.
- Require within project methodologies that projects refer to the Lesson Learnt knowledge base, and formally capture and disseminate lessons learnt within the project up to governance bodies for visibility. This will enhance the Ministry's opportunities to evolve the learning culture associated with change initiatives.

Consider privacy early

Status: Progressed

The Ministry is implementing a Privacy, Human Rights and Ethics framework (PHRaE). A particular focus is on embedding privacy thinking early into new initiatives as they are being formulated. The PHRaE has been trialled across a number of projects to further refine it.

The Ministry is focused on updating its Privacy operating model to support the delivery of the new framework including greater resourcing to support the business with Privacy expert advice. Towards this, the Ministry is in the process of recruiting additional Privacy specialists, and has used external consultants to support the development of its Privacy capabilities. It is important for the Ministry to develop and sustain internal capability and expertise in Privacy, as well as, to leverage and transfer the knowledge of contract resources to internal staff.

The three projects that were sampled, have confirmed that they have worked closely with the Privacy function and that there has been strong senior leadership awareness and engagement with Privacy matters including with the new PHRaE framework. The projects have either completed a Privacy Impact Assessment or a Privacy Questionnaire, and a Privacy advisor has worked with them to provide subject matter input so that sound consideration of relevant Privacy elements is able to occur.

The Privacy function has also improved its ability to track the number, quality, and timeliness of Privacy Impact Assessments, and is working with the CISO function to identify initiatives that require Privacy input.

While Privacy considerations and recommendations are being raised within the projects, the Ministry needs to have formal tracking and validation that the recommendations have been undertaken prior to project go-live.

Recommendations:

- Continue the rollout and investment into the PHRaE framework and the operating model required to support it. This includes investing in internal resourcing and having knowledge transfer occur from contractor resources so that the Ministry can develop and sustain internal Privacy capability.
- Implement a process and the requirement to confirm that key Privacy recommendations are implemented prior to project go-live.

Validate information security risk mitigations

Status: Progressed

The Ministry has strengthened its process to validate security controls (mitigations) through updating of its security Certification and Accreditation process. This is being embedded and includes:

- The implementation of a formal controls validation approach and report (Controls Assessment Report) for systems that require a full Certification and Accreditation (the highest level of security risk). The Controls Assessment Report documents which controls should be tested prior to going live and documenting the results from the testing. For medium risk systems, key controls are required to be validated but a Controls Assessment report is not required. For low risk systems, controls are confirmed with control owners but are not required to be formally validated.
- For the Controls Assessment Report, the Ministry has developed guidance on the control testing approach and what percentage of controls are to be validated based on control grades. This Controls Assessment Report is required to be signed off by the CISO and the Business Owner of the respective project and is referenced as part of the final Certification and Accreditation approach.
- An application (Risk and Controls Application (RCA)) has been developed to provide visibility of controls to the control owners.

- In addition to the controls validation of new projects, the Ministry has been auditing controls that have been identified, and assessing if the controls are active and operating, with the aim of implementing any outstanding controls.

The controls validation approach is currently being embedded across the business and within projects. Through our interviews with the three projects, we noted that the project teams' understanding of controls validation was heavily reliant on penetration testing. We did observe for two projects that controls validation had either been completed or was in progress. For the third project, it was too early within the project lifecycle for controls validation activities to be completed.

The new guidance that has been developed is clear on the various types of evidence required to validate a control. However, we observed controls validation for a medium risk project heavily referring to items documented within the design documentation as a method of demonstrating that a control is in place. We would reinforce that the better approach to controls validation would to sight / directly walkthrough or test that the control is in place and operating within what has actually been built, configured, and deployed – through direct technical or process validation, instead of reviewing what is *documented* about what is deployed.

Recommendations:

As part of embedding the controls validation approach:

- Educate projects (and team members within projects) that controls validation goes beyond just undertaking penetration testing.
- Reinforce the need for evidence of a control being in operation beyond references to the design or other documentation as the method to validate controls. Better methods include directly validating technical and process inputs and outputs (for example, validating system configuration, or logging of events operating effectively through sighting the events that are captured when specific actions are taken on a system),

Further Thoughts

To assist the Ministry in realising greater value from its investment in Privacy, Information Security, and consistent and robust project delivery disciplines, it is important the Ministry assign central ownership for the completion of the work programme to embed the lessons across the organisation. Considering the importance of Privacy within many of the Ministry's initiatives, the Chief Privacy Officer may be the appropriate person to own this – thereby making sure that the Ministry remains focussed and delivers the intended outcomes through completion of the work programme within the 12 month overall timeframe.

For an organisation with the scale and profile of the Ministry it is important to continue to evolve its learning and continuous improvement culture so that risk to the Ministry and its clients can be reduced through high performing change delivery. Building on from the senior stakeholder engagement in the work associated with the rollout of the new PHRaE framework, it is important that from a governance perspective the senior stakeholders for change initiatives sustain this engagement. This would include modelling the embedding of the framework within their teams' hearts, minds and activities; and satisfying themselves independently that the right things are being done in terms of Privacy, Information Security and project delivery disciplines for the change initiatives they lead.

In another 6 to 9 months, the Ministry should undertake an internal assessment (through the Ministry's Risk and Assurance function) on its progress on completing the work programme to implement the lessons and associated recommendations and the extent to which those have been institutionalised across the Ministry.

Appendix A: Terms of Reference

Follow-up review of the Independent review of the Ministry of Social Development's decisions relating to the IT system used to capture individual client level data

24 November 2017

The Chief Executive of the Ministry of Social Development (the Chief Executive) has commissioned a follow-up review of the independent review of the Ministry of Social Development's decisions relating to the IT system used to capture individual client level data that was completed in May 2017 by Murray Jack together with Anu Nayar, Deloitte NZ National Leader of Cyber, Privacy and Resilience, and Adrian van Hest, PwC, National Cyber Practice Lead.

The follow-up review will be led Anu Nayar.

Objectives of the follow-up review

The objectives of this review are to follow-up on the lessons to be learnt and recommendations outlined in the 12 May 2017 report to assess the progress the Ministry has made in implementing these lessons and provide advice on what, if any, further actions are required to ensure these lesson continue to be embedded.

Matters in scope

The review will consider the progress the Ministry has made in implementing the lessons learnt outlined in the May report and provide advice on any further actions that may be required to further embed these changes. In particular the review will consider how the Ministry has:

- gathered and leveraged off the knowledge and experience from other users of the Shared Workspace in a more structured manner.
- applied formal project disciplines consistently to ensure appropriate checks and readiness approvals for deployment.
- considered privacy early.
- validated information security risk mitigations.

Matters out of scope

- the current individual client level data process and supporting systems used by the Ministry.
- other uses of the Shared Workspace.
- processes and systems under the responsibility of Oranga Tamariki.