Deloitte.

Ministry of Social Development

Independent Review of Information Systems Security

Phase 2

Review of Wider Information Systems Security

30 November 2012

Contents

Executive summary

Confidence that information is secure is vital to the trust-based relationships needed to provide effective services

The Ministry of Social Development ("the Ministry") is New Zealand's largest government department providing services to more than 1.1 million clients, receives in excess of 230,000 calls a week, and approximately 40,000 online applications a month. The Ministry provides services to those in need, helping them become successful in their lives. These services are complex and information is vital to their effectiveness. No matter what levels of physical and system protection are in place, security breaches as a result of system failures and human error may occur. Nonetheless, individuals should expect that all reasonable efforts are made to provide physical and technical environments that ensure personal information is secure from unauthorised access and use.

Recent years have seen global and rapid change in how services are delivered. Like many organisations in New Zealand, the Ministry has implemented new ways of interacting with its clients and stakeholders, all of which rely on exchange of information. This trend will only intensify in the future.

Objectives of the review

Public confidence – and more importantly the confidence of the Ministry's clients – in the Ministry's management of information security and information privacy were eroded by the security breach in October 2012. The Ministry commissioned an independent review of its information systems security to understand what occurred and to help restore the level of confidence and trust that is needed.

Phase 1 of this review, which investigated the circumstances of the "kiosk" security breach, was completed in early November and identified three primary causes of the security breach.

This second phase of the review seeks to answer two key questions:

1. Are the primary causes identified in Phase 1 evident across the Ministry and therefore pose broader risk?

2. Taking a broader perspective, are there other weaknesses in the Ministry's approach to information security that pose risk?

Conclusions of the review

Are the primary causes of the security breaches identified in Phase 1 evident across the Ministry?

We assessed the Ministry's information security approach to understand whether the primary causes we observed in the Phase 1 review are evident across the Ministry's current business as usual and project activities.

Security was not adequately designed into the "kiosk" architecture and deployment approach.	From what we have observed, this primary cause is **not evident across the Ministry**. However, the information security management structures that are in place need to be strengthened to give leadership a high degree of confidence that this primary cause does not emerge to create issues elsewhere. In particular, explicit review and decision rights need to be established in the project lifecycle to ensure that security requirements are consistently met.
The exposures identified within the penetration test report were not appropriately addressed and followed up.	From what we have observed, this primary cause is **not evident across the Ministry**. Follow up on security testing is common practice. However, oversight of information security risks and security related activities need to be strengthened to give leadership a high degree of confidence that this primary cause does not emerge to create issues elsewhere. For example, all security testing reports should be provided to an appropriate management level, follow-up activities and resolutions should be formally described and agreed, and strong information security expertise should be applied to understanding the implications of findings and any residual risks.
The risk management processes did not effectively escalate security exposures to management, nor ensure appropriate mitigating actions were taken.	From what we have observed**, the policies and processes at the time did not explicitly require all security risk exposures to be escalated to management. Consequently, this led to this primary cause being evident across the Ministry**. Recently, the Ministry has taken steps to ensure that the governance bodies of projects receive full project risk registers, which, combined with the strongly positive culture towards information security, and the heightened awareness of information security risks, we expect to satisfactorily mitigate this weakness. In addition, greater structure and discipline needs to be applied to information security risk management to give leadership confidence that it is appropriate and robust – for example, ensuring that subject matter expertise is applied to information security risk identification as well as information security risk management, and that information security risks across the organisation have a clear escalation path.

In summary, two of the three primary causes that led to the "kiosk" security breach in October 2012 were not found to be evident across the Ministry, whilst the third primary cause was found to be evident across the Ministry. A number of actions have been identified by the Ministry and as a result of this review that would strengthen the Ministry's information security approach.

Taking a broader perspective, are there other weaknesses in the Ministry's approach to security that pose risk?

There are other weaknesses in the Ministry's approach to security that pose risk. In our experience, these weaknesses are not unusual for New Zealand organisations. In isolation, each weakness does not present a high level of risk, and our findings do not suggest that the degree of risk within the Ministry is higher than within many similar organisations.

Based on the work we performed within the scope of our review, we found no evidence to indicate that the weaknesses described above have resulted in breaches of security vulnerabilities within the Ministry. However, we would expect that, as part of implementing the recommendations of this review, the refresh of the Ministry's risk framework currently in progress, and through undertaking the improvements already underway, any potential high-risk vulnerabilities would be addressed. Furthermore, the Ministry is committed to working through the process in full for the GCIO Review of Publicly Accessible Systems.

Taking a sound approach to information security and privacy requires finding an appropriate balance – involving a series of decisions and trade-offs to enable the balance of absolute priorities such as the protection of client personal information, effective and undisrupted service delivery, delivery of a significant programme of legislative driven change, and at reasonable cost.

Hence, because of the importance of the services the Ministry operates and the ever increasing demands it faces - including the push for increased online services and "self-service" delivery, the current level of information security management needs to be improved to better serve the Ministry's current and evolving needs. Also, this will be integral in restoring trust and confidence with the Ministry's clients, the public and external stakeholders.

While a lot of the right building blocks to manage information security are in place, these need to be formalised, led at a senior level, and expanded.

The Ministry has made significant progress to strengthen its approach to information security and information privacy in recent years. This has established many of the building blocks that are needed to manage information security risk effectively.

In addition, the Ministry has a strong culture that clearly understands the importance of privacy and security. This culture has meant that good judgment has generally been applied, even in the absence of more formal structures. The Ministry has also demonstrated a positive willingness to learn the lessons of the October security breach. The Ministry's programme of work to improve its information security approach post October, has further demonstrated commitment to restoring confidence and trust.

However, more needs to be done to achieve and maintain an appropriate approach. While information security is considered in many parts of the organisation, approaches and tools are often informal or lack specificity. This places too much reliance on the capabilities of individual people.

Governance and organisational structures	Leadership and accountability for information security needs to be formally assigned to a senior level within the Ministry, and the organisational structures need to be aligned under that leadership so that responsibilities are clear and activities are prioritised, well-managed and coordinated.
Frameworks and approaches	Strategy, business plans, policies and approaches need to be enhanced and linked so that they are comprehensive in coverage, consistent and sufficiently detailed to support decision making. This needs to include clear definitions of what 'success looks like' for information security, supported by appropriate metrics and targets.
Execution and assurance	Existing processes for information security need to be enhanced and redesigned to ensure that the appropriate activities are carried out. This needs to include implementation of appropriate independent assurance to monitor general business compliance with information security requirements, and to provide confidence that information security activities and controls are adhered to and effective.

Maintaining effective information security is an on-going process

The rate of change is likely to continue as the Ministry continues to seek new ways of being more client-focussed, making it easier for people to access the services they need. Increasingly, the push for "self-service" functionality and the digitisation of services also means that the service delivery environment is now intrinsically reliant on secure and resilient systems, data and processes. This also emphasises the changed risk landscape where now, there is an on-going need to keep refreshing how personal information is protected. Information security management cannot sit still in this dynamic environment. As new threats and opportunities emerge, the capabilities required to manage information security well are becoming more demanding. This means that information security needs to be led from the top so that what an organisation does to respond to threats and opportunities is integrated with business strategy and operationally aligned.

Information security may seem like a technical subject, but it is really a business issue that requires broad thinking and skills – from business objectives to how these are achieved operationally, and what technical solutions and controls need to be in place. It also needs to be a dynamic discipline, which requires constant awareness of the changing risk environment and on-going investment to ensure the right level of capability is maintained. What is fit for purpose today will likely not be fit for purpose tomorrow, hence requiring the commitment to evolve and the capability to respond to emerging needs.

Next steps

The Ministry is currently participating in the GCIO Review of Publicly Accessible Systems, which will make public sector wide recommendations on improvements to the security of publicly accessible systems.

The Ministry should continue the information security improvements that are already underway, and consider and implement the detailed recommendations of these reviews.

We expect that by formally assigning information security management to the appropriate senior level within the Ministry, appropriate implementation of the recommendations of this review, and working through the full process of the GCIO review, the Ministry will have confidence in its approach to information security.

Introduction

Background to the review

On 14 October 2012, a member of the public alerted the media and the Office of the Privacy Commissioner to a security issue with the "kiosks" that the Ministry had been providing to clients at Work and Income Service Centres.

In response to the information, the Ministry ceased providing "kiosk" services, engaged with the Office of the Privacy Commissioner and other stakeholders, issued a Terms of Reference for an Independent Review of the Ministry's Information Systems Security on October 17, and established an independent Steering Group to govern the review.

The Ministry has also commenced a series of information security improvements, and these are summarised in Appendix C.

Terms of Reference

Phase 1 of the review was completed on 01 November 2012, and investigated the circumstances and causes of the "kiosk" security breach.

Phase 2 of the review is focused on the Ministry's wider information systems security, including the policies, governance, capability and culture. The objective of the review is to make recommendations about the actions that need to be taken to restore and increase public confidence in the Ministry's information systems security.

The Terms of Reference for the Independent Review is included in detail in Appendix A.

Purpose of this document

This document presents the Phase 2 report of the Independent Review.

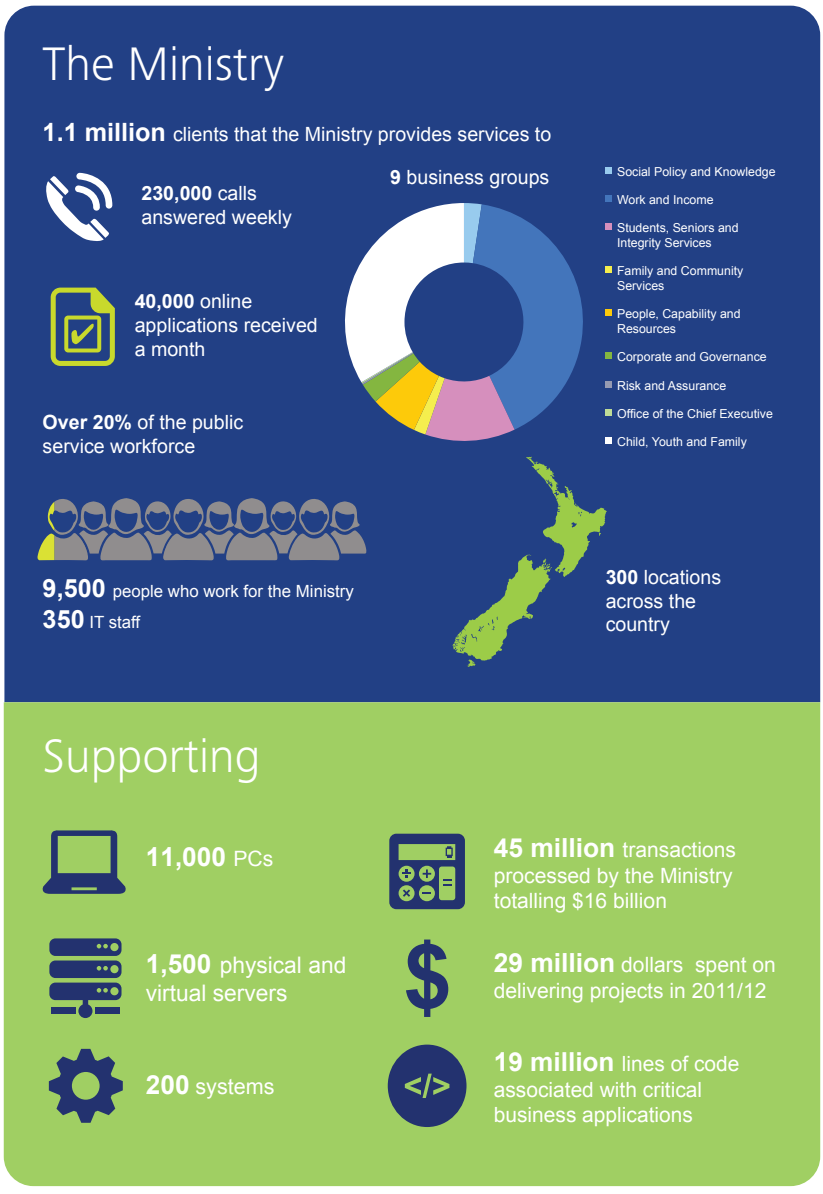
In particular, its purpose is to provide recommendations to the Ministry's Chief Executive on what needs to be done so that the Ministry can have confidence that its approach to information security is appropriate. Having that confidence is fundamental to restoring and increasing public confidence in the Ministry's information systems security.

In parallel with this work, the Ministry is currently participating in the GCIO Review of Publicly Accessible Systems, which aims to provide Ministers with assurance on the security of publicly accessible systems, and Chief Executives with advice on security improvements which can be made in the deployment and operation of such systems. Phase 2 of this Independent Review of the Ministry's Information Systems Security has not sought to duplicate any of that work.

The Ministry environment

The Ministry is a large and diverse organisation that needs to manage complex business processes and significant transaction volumes, at the same time as delivering extensive change initiatives. Additionally, in the period following the Canterbury earthquake, between February 2011 – June 2011, 120 staff from the Ministry's IT function of approximately 350 staff, spanning key areas including senior members of the management team, were dedicated to the work in Canterbury. While the impacts are not as high now as they were during that period, the Ministry continues to provide support to the Canterbury earthquake recovery efforts, in addition to its on-going service delivery and change programme demands.

The following diagram provides a high-level overview of the Ministry environment.[1]



[1] This information was provided by the Ministry.

Approach

Key questions

We have sought to answer two key questions:

> *1. Are the primary causes identified in Phase 1 evident across the Ministry and therefore pose broader risk?*
>
> *2. Taking a broader perspective, are there other weaknesses in the Ministry's approach to information security that pose risk?*

For context, Phase 1 of the review identified three key causes of the "kiosk" security breach:

- Security was not adequately designed into the "kiosk" architecture and deployment approach.
- The exposures identified within the penetration test report were not appropriately addressed and followed up.
- The risk management processes did not effectively escalate security exposures to management, nor ensure appropriate mitigating actions were taken.

What is information systems security?

In this review, we have considered information security overall, because it is generally difficult to isolate information systems security aspects. Also, most aspects of information systems security of an organisation tend to be delivered through use of an overarching information security approach, as was observed in the Ministry as well.

In the context of this report, information privacy is a major strategic issue that drives information security, and is one of the key outcomes that is aimed to be delivered by a sound approach to information security.

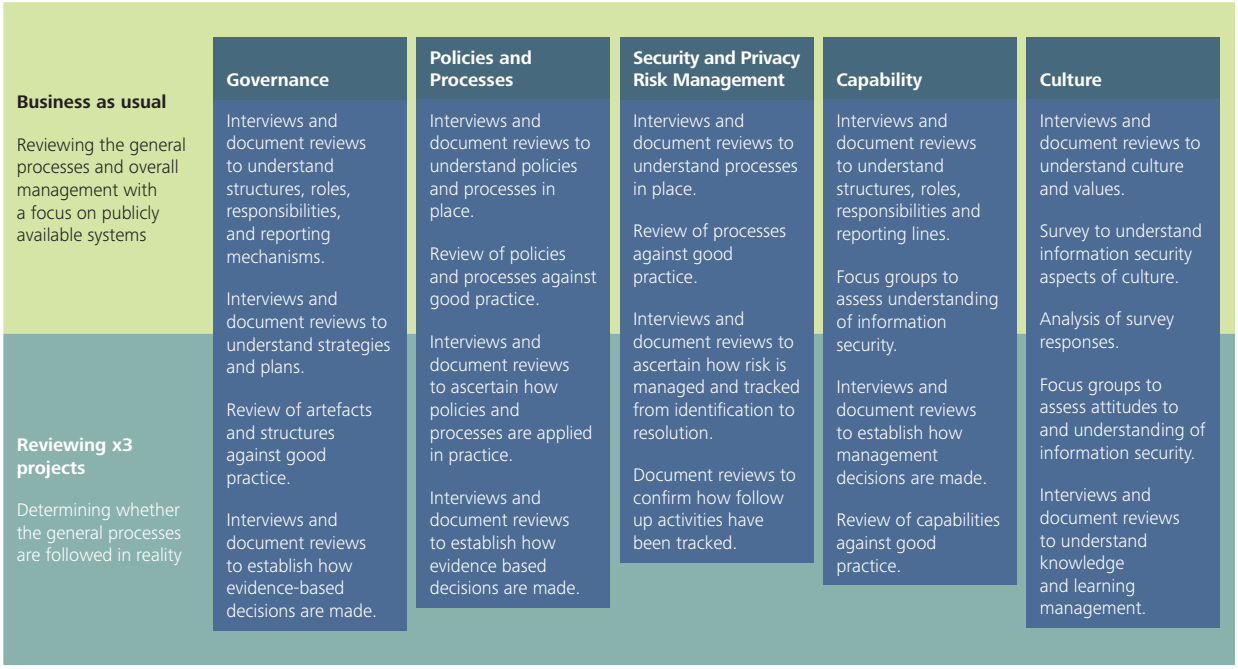
We have also considered wider information management and protection elements and where applicable, physical security aspects relevant to the protection of information or systems.

We have applied the following definitions relevant to information security, of which information systems security is a subset:

Information security	Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, recording or destruction. Information security is closely related to information privacy.
Information privacy	The set of actions and decisions an agency makes on how it uses, handles and looks after personal information given to it.
Information management	The collection, handling and distribution of information from one or more sources for use within the business so that information is treated as an asset.
Physical security	The measures used to prevent unauthorised people from physically accessing a building, facility, resource, or stored information, and the wider measures that can be used to detect and respond to such attempts. It also pertains to physical safety.

Five perspectives applied for this review

We have assessed and made observations about the Ministry's approach to information security for both business-as-usual operations[2] and projects across the following five perspectives. The following diagram outlines our approach to assessing the five perspectives for business as usual operations and projects.



For business as usual operations, we reviewed how the Ministry approaches information security within its day to day service delivery activities. This was done using a variety of methods such as, interviews, documentation reviews, walk-throughs and observation, and for review of the culture perspective, review of internal surveys, and conducting surveys and focus groups.

For projects, we selected three projects to understand the Ministry's information security approach towards change initiatives. The sample was selected from a candidate list with the criteria that the duration of the project is greater than 3 months, is a representation of initiatives involving the major service lines, includes some form of external interaction, and project initiation was within the last two years.

For each of the perspectives across the Ministry's business as usual operations and selected projects, we reviewed a number of dimensions to formulate a more complete view of the Ministry's approach to information security.

[2]Business as usual operations means the day to day activities involved with the Ministry's delivery of its services

Review Framework:

Governance	Policies and Processes	Security Risk Management	Capability	Culture
• Strategy • Leadership and decision making • Accountability • Investment • Monitoring and oversight	• Enterprise support functions • Process effectiveness and control • Compliance • Information management • Lifecycle approach (projects) • Process design (projects) • Transition from projects to business as usual	• Risk identification • Risk evaluation • Mitigations and treatments • Escalation, monitoring and reporting • Risk appetite	• Structure • Roles and responsibilities • Expertise • Management • Enablers	• Awareness, understanding and communication • Values • Learning and adaptive • External focus • Risk intelligence

For each of these elements, we have considered:

- Whether the systems (processes, guidance, policies etc) that are in place are fit for purpose.
- Whether the systems, where they are in place, are complied with.
- Whether actual practices carried out are appropriate.

In this context **fit for purpose** *means that the system must be designed to cope with the Ministry's particular environment and reduce the likelihood of failure to a level that is reasonable in light of the severity of the potential consequences. It is not reasonable to expect that the probability of failure is reduced to zero.*

More information on the work performed is included in Appendix B.

Disclaimer and limitations

This report is prepared in accordance with the specific terms of reference between Deloitte and the Ministry of Social Development ("Ministry"), and for no other purpose. Other than our responsibilities to the Ministry and the Steering Group for this review, neither Deloitte nor any member partner or employee of Deloitte accepts or assumes any duty of care or liability to any other party in connection with this report or engagement.

The report is based upon information provided by the Ministry and interviewees. Deloitte has reviewed, and relied upon this information. Deloitte has assumed that the information provided was reliable, complete and not misleading and has no reason to believe that any material facts have been withheld.

Accordingly, neither Deloitte nor its partners, directors, employees or agents, 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 views provided in this report resulting directly or indirectly from any such circumstances or from any assumptions upon which this report is based proving unjustified.

This report dated 30 November 2012 was prepared based on the information available at the time. Deloitte has no obligation to update our report or revise the information contained therein due to events and information subsequent to the date of the report.

Acknowledgments

We have had the full cooperation and assistance of the Ministry's staff and management team throughout this review.

We acknowledge and appreciate the input and guidance contributed by external stakeholders to the review.

Business as usual information security

Introduction

The Ministry is New Zealand's largest government department providing services to more than 1.1 million clients. It receives in excess of 230,000 calls a week, and approximately 40,000 online applications a month. As a large organisation that delivers a broad set of services to clients, the Ministry operates many systems and processes that deal with information – much of which is of a personal and sensitive nature.

This has the potential to expose the Ministry to a range of information security and information privacy risks, such as inappropriate internal access to information, accidental release of client information to the wrong parties, and unauthorised external access to information. There are more potential information security and information privacy risks posed through recent initiatives that have increased access to services and information to clients and partners, for example via Ministry websites, and a major push for "self-service" functionality. The trend – driven by client, public and Government expectations – is for even greater access to information, stronger integration with other information and more personalised service. This means that the Ministry's information security and information privacy risk profile will continue to evolve.

The importance of protecting personal and sensitive information is well understood and accepted within the Ministry, and is formalised in the Code of Conduct. Since about 2006, the Ministry has been increasing its focus on information security to develop plans and practices in response to increasing proximity of information systems to the public (e.g. online access) and the consequent increase in risk. This has included development of a security strategy within the IT function as well as a roadmap for strengthening information security.

A range of business areas are involved in information security activities, including:

- Architecture Team within the IT function
- IT Security Team
- IT Infrastructure and Services
- Information Services
- Legal Services
- Teams within operational business units

Broadly, these activities cover policy development, IT operations (e.g. patching), managing access to business applications and information, and privacy awareness and training.

Key Findings

The key findings below relate to one or more of the perspectives we assessed the Ministry's information security approach against.

Information security is not explicitly considered within existing governance arrangements. ***(Governance)***

The Ministry has robust governance structures in place, but these do not consider information security explicitly. For example, executive-level strategic planning and performance monitoring does not include information security.

Therefore the planning and monitoring activities that occur are difficult to link back to overall strategic objectives, inconsistent, and difficult to prioritise.

The team structures relating to information security do not reflect increasing demands. ***(Capability)***

Responsibility for information security is distributed across several different teams in different parts of the organisation (e.g. various support functions). This makes it difficult to ensure that activities are coordinated. It increases the difficulty in prioritising work effort because overall demand and capacity are not understood.

Without clear visibility at the leadership level of issues that are being addressed, and guidance on priorities, this creates the risk that security management is reactive at an operational level, rather than proactive in support of overall objectives.

There is no enterprise-wide approach to information security risk management. ***(Policies and Processes, Security Risk Management)***

Some appropriate elements are in place (such as processes, frameworks and work practices) but these have not been consolidated and expanded to provide a cohesive and comprehensive set of guidance and tools.

This means that activities and investments are not managed in a consistent and clearly understood manner, placing greater reliance on individual judgment. While there is strong general awareness of the importance of information security, staff lack detailed information to support decision-making and work prioritisation.

Performance measures and target outcomes for information security are not defined. ***(Governance, Capability)***

While there is some monitoring and reporting of security-related metrics, the required performance has not been defined at a strategic level, nor have they been specified as operational targets. This means that teams lack adequate top-down goal definition to guide their work and prioritisation. It also means that there is no structured basis for establishing the return on investment for information security activities, which makes it more difficult to make robust value-for-money decisions on resources committed to such activities.

Visibility of information security controls and assurance over the business as usual environment is limited.

(Policies and Processes)

Because of the lack of explicit definitions and priorities, and the involvement of several teams within the Ministry, an overall view of controls, assurance and effectiveness cannot be determined. This means that improvements made to what and how work is carried out are tactical and achieve value in specific pockets, rather than optimising results for information security overall. This also means that a current picture of where the Ministry stands in relation to Government security standards is difficult to maintain.

The Ministry has a strong culture that values the importance of privacy and information security.

(Culture)

People at all levels within the Ministry are highly aware of the importance of information security in the context of protecting information privacy (refer to Appendix E for insight obtained from the culture survey). This culture has meant that practical and sound judgment has been applied to mitigate risks in many instances, even in the absence of more formal frameworks and tools. Stronger Ministry-wide education would support more consistent and effective application of security principles in practice. When combined with the strong culture towards the topic, this provides a good basis for improvement.

Mechanisms to maintain a view of the information security risk profile are not in place.

(Policies and Processes, Security Risk Management)

A general transition process from projects to business as usual operations is in place and well-established. Because information security is not an explicit consideration in this process, there is no structured and consistent way to understand and capture the overall net risk impact of changes that are implemented.

This means that an accurate view of the information security risks inherent in the environment at any point in time cannot be maintained. As a result, progress to improve information security is difficult to measure, and risk mitigation actions need to be prioritised somewhat subjectively.

Alignment with external requirements.

(Policies and Processes)

While many in the Ministry are aware of the NZISM, the NZSIGS and other Government security requirements, there are no existing processes to mandate compliance on any aspect of these standards. Further, the lack of clear guidance on how organisations should consider and determine which of these requirements, how they apply to them, and how best to meet them, poses a challenge on how these are addressed, including at the Ministry.

We note that post the “kiosk” security breach in October 2012, the Ministry has established specific practices to require alignment with the Government requirements for any new externally accessible applications. We understand an internal review to determine current status in relation to compliance with Government security related requirements is underway.

Various information security practices and controls are in place across the Ministry. There is limited visibility and no formal monitoring of the overall status of information security compliance across the organisation because the various activities are not joined up.

Information privacy practices appear to be well defined and consistent.
(Policies and Processes, Culture)

The Ministry of Social Development's Code of Conduct is well socialised, communicated and embedded within the Ministry. It includes clear coverage of information privacy, security and integrity themes.

We observed strong induction practices across the Ministry that included coverage of information privacy elements.

Legal Services, Procurement and Risk and Assurance all serve a role in fostering awareness and contributing as part of the Ministry's activities to embed strong approaches to information privacy. They also support business involvement and approaches on information privacy requirements, and serve as advisors to the business groups on this topic.

We also found through our review of culture that people across the Ministry echoed the sentiment that they respect and take information privacy of client information as an absolute requirement.

There are opportunities to leverage these successes more broadly to incorporate information security.

Recommendations

Assign Deputy Chief Executive (DCE) level leadership and accountability for information security.

This will formally assign information security management to the appropriate senior level within the organisation and provide a single point of responsibility for driving information security activity across the Ministry. While we acknowledge that all leadership team members will play a part in the on-going improvement of the Ministry's information security approach, this DCE will be accountable for ensuring it happens. We would expect this senior role to be supported through the establishment of a clear governance structure for information security matters.

The DCE should lead implementation of the remaining recommendations in this report and provide progress reporting to the broader leadership team.

Information security activities and performance objectives for key teams involved in these activities, should be coordinated, and have clearly defined links back to this senior role, while work to develop the right long-term operating model for information security is carried out. That operating model should include:

- Architecture
- Policy
- Operations
- Management
- Innovation and learning
- Assurance and quality management

The information security function for the Ministry should be kept distinct (and separate) from the Chief Information Officer function so that the benefits of an appropriate level of challenge and wider business perspectives on information security and privacy can be achieved.

We note that the Ministry has already commenced preliminary thinking on this matter and is taking actions to move this forward.

Integrate information security into strategic planning and performance monitoring.

This work should build on the plans already developed – for example within the IT function and Information Services – to create a comprehensive strategic platform for information security management, which is clearly aligned to the Ministry's business strategy.

This should include:

- Confirming clear strategic objectives for information security
- Establishing the changes and actions needed to achieve the objectives
- Developing a roadmap of initiatives to implement the changes and actions, with agreed timeframes, accountability and funding – for example, a 100 day plan for more immediate actions and a 12 month plan for the initial set of strategic objectives
- Establishing metrics and performance targets that cascade from strategic measures to an operational level

- Establishing a monitoring and reporting approach that demonstrates progress on the strategy and tracks performance over time

It also provides an opportunity to drive broader awareness across the organisation of information security and what it means in practice.

The work will provide top-down guidance and priorities for managing and carrying out information security-related work.

Improve information security risk management, control and assurance approach.

This should build on the teams, capability and artefacts that are already in place. It should formalise and align the organisational structure, and remedy gaps in current approaches, frameworks and expertise.

An important step to improving the approach will be developing an accurate and comprehensive view of the organisational level of information security risk. We recommend that this should be achieved through a detailed risk analysis of the current environment, and putting in place the mechanisms needed to maintain the currency of the assessment as changes are made to the business environment.

An enterprise-wide approach to information security should be developed, and this should cover three lines of defence:

- **Day-to-day risk management and control** – how risk is managed and mitigated at an operational level
- **Risk oversight, policy and methodologies** – the tools and processes in place to guide operational activity and risk management
- **Independent assurance** – the means to review, test and ascertain effectiveness and compliance

All three lines of defence should reflect relevant external standards and good practices. An effective approach would include incorporating appropriate information security and information privacy considerations into the work being done to refresh the Ministry's risk framework currently underway. This will enable the existing enterprise risk management structures within the Ministry to be extended to include information security and information privacy risk matters effectively.

These activities include providing guidance on how the Ministry will consider risks and opportunities related to privacy and information security.

Appropriate teams and roles should be coordinated and where required, refreshed to more effectively manage information security. This should consider how to leverage other support functions and lead business engagement, and how linkages with projects need to be managed. It will provide clear responsibilities and enable coordination of information security activities across the Ministry to ensure that resources are applied to the right priorities.

Projects information security

Introduction

The Ministry is a large and diverse organisation with a correspondingly large and diverse set of projects running at any one time. These range from major policy-driven transformation programmes (such as the Welfare Reform Programme) to standard IT infrastructure upgrades.

Projects are governed by steering committees which vary in size and make-up, and usually include General Manager or Deputy Chief Executive level membership.

Projects with an IT component are delivered according to a defined project management process supported by the IT PMO and IT Work Management Centre. This process covers the entire project lifecycle from concept to handover to production. Project staff for IT-related roles are drawn either from internal pools (such as Java developers, testers and architects), consulting organisations (usually through standing support arrangements) or from the contractor market. Other roles are filled by people from the wider organisation. Non-IT projects do not follow the same standardised project approach.

IT projects follow a range of software development methodologies including variations on traditional waterfall and agile approaches. The projects sometimes add new components to the technology environment, and sometimes add or modify external access channels.

A large proportion of the Ministry's change effort is driven by legislative requirements and the accompanying deadlines for those requirements, creating significant demands on the Ministry.

Appendix D illustrates points during the project lifecycle where security input is obtained.

Key Findings

Information security governance and responsibility on projects is not well-formed.

(Governance, Policies and Processes)

An Architecture Review Board (ARB) is in place, which reviews security at the architectural level, although it has no specific mandate to do so. Further, the ARB does not have a formal mandate for enforcing its decisions, and there are no formal structures in place to ensure that projects engage appropriately with the ARB.

The Ministry's IT Security Team also often plays a role on projects, for example commissioning penetration testing. However, the requirements for their involvement are not clear and the team does not have a mandate to direct projects to take particular approaches and actions in response to any issues. The team is not consistently involved early in the project lifecycle.

Overall, it is not clear who is accountable for security at a project level. With the ARB and IT Security Team in place but with informal or limited roles, there is a risk that projects implicitly rely on them to manage security and, consequently, fail to establish appropriate ownership and resources.

There are insufficient formal requirements to consider information security within the project lifecycle.

(Governance, Policies and Processes, Security Risk Management)

Information security is incorporated consistently within the architectural design aspect of the project lifecycle, but there is a lack of formal requirements to consider security in other phases and aspects of projects, including transition to business as usual. Security risk assessments are not mandated. This means that business cases and budgets do not necessarily account for security-related effort, which can result in project delays and cost overruns when security work is added into projects later.

Information security guidance is limited to requirements within the non-functional requirement template. This leaves it up to projects to determine whether to include functional security requirements during design, software development and testing – with inconsistent results.

There is insufficient information security expert involvement in projects.

(Policies and Processes, Capability)

A security architect provides security input to projects through the ARB and sometimes directly. However, solution architects without security expertise are frequently expected to identify security risks. Based on the nature of the project, and its resource composition, the IT Security Team may become involved with a project, primarily to manage penetration testing near the end of the project lifecycle.

This means that the Ministry relies to a high degree on the judgment of key project personnel to seek the right level of expertise and input.

Education on security principles and practices relevant to project related activities is inadequate.

(Governance, Policies and Processes, Capability, Culture)

A core value within the Ministry is to keep client data private and secure, and Ministry staff and long-term contractors bring this value into their project teams. However, this culture is not

effectively translated into project activities due to a lack of guidance and education on the practical application of security principles.

Consequently, there is no common understanding of security to inform the management and governance of projects, including the management of security risks. This leads to inconsistent levels of oversight and risk acceptance.

The Ministry is becoming more reliant on external project assistance, but induction training or on-boarding practices for contractors being brought in to do work for the Ministry do not occur or occur inconsistently across various teams in the Ministry. These do not cover information security expectations. This means that unlike many of the Ministry staff who have developed extensive institutional knowledge about the Ministry's environment and way of doing things, including the cultural emphasis on protecting client information, they may not have as much guidance on these expectations. We found it to be similar for non-project areas across the Ministry.

Project security risk evaluations do not occur consistently.

(Policies and Processes, Security Risk Management, Capability)

Security risks and exposures are not adequately assessed, shared and accepted within the wider organisation during project acceptance and transition to business as usual. The implicit risk is increased by projects assuming that the existing platform is sound, which means that there is no structured assessment of the 'net risk' impact that a project has on overall information security.

Recommendations

Establish more explicit information security review points in the project lifecycle.

The project lifecycle (for IT and non-IT projects) should include information security explicitly at key decision points. For example, approval of requirements should include acceptance of the security aspects, and business acceptance criteria for go-live should include acceptance of security testing and residual risk.

Explicit decision and approval rights should be introduced into the project lifecycle to ensure that accountability for these decisions is clear, decisions are consistent, and decisions are informed by an organisation-wide perspective of information security risk. These rights must reflect the accountability of different roles (e.g. project manager, IT Security team) for different aspects of information security.

Because not all projects carry the same level of risk, this should include risk evaluations at key points in the project lifecycle (including prior to the business case approval) to determine the appropriate level of security activity and oversight for each project. This will help ensure that additional controls are applied in a 'fit-for-purpose' approach, rather than in a blanket approach that could well affect service delivery performance or impose unnecessary overheads such as time, cost, people, process and technology load. This recommendation includes non-IT projects that are not currently covered by the IT PMO, and awareness training in the methodology for key stakeholders such as members of Business Steering Groups.

Expand current processes for formal project acceptance and handover to business as usual to require security as an element.

Provide more guidance on information security in the existing project methodology and project documents and templates.

This will strengthen awareness of project team members and the quality of deliverables produced over the project lifecycle. For example, we would expect that it includes appropriate prompts to consider information security and reference to the Ministry's tools, approaches and expert personnel. It should also set out formal requirements for the involvement of the IT Security Team and other (internal or external) security experts.

Use of a knowledge base would improve on-going refinement of practices and disseminate knowledge and experience.

Enhance project management and delivery.

The level of information security awareness of existing teams should be improved. This includes awareness of information security concepts and the Ministry's expectations, processes and sources of expertise. In particular, explicit decision and approval rights on security matters throughout the project lifecycle need to be established and formalised.

This should consider appropriate integration, reporting and knowledge sharing with business as usual operations aspects of information security teams. A training needs evaluation should be carried out to identify expertise gaps – across information security teams, the project resources within the Ministry, and business managers involved in providing guidance or governance to projects. This can then be used to develop appropriate training plans to strengthen capabilities while not going overboard.

Conclusions and recommendations

Are the primary causes of the security breaches identified in Phase 1 evident across the Ministry, and therefore pose broader risk?

We assessed the Ministry's information security approach to understand whether the primary causes we observed in the Phase 1 review are evident across the Ministry's current business as usual and project activities.

Security was not adequately designed into the "kiosk" architecture and deployment approach.	From what we have observed**, this primary cause is not evident across the Ministry.** However, the information security management structures that are in place need to be strengthened to give leadership a high degree of confidence that this primary cause does not emerge to create issues elsewhere. In particular, explicit review and decision rights need to be established in the project lifecycle to ensure that security requirements are consistently met.
The exposures identified within the penetration test report were not appropriately addressed and followed up.	From what we have observed, **this primary cause is not evident across the Ministry.** Follow up on security testing is common practice. However, oversight of information security risks and security-related activities need to be strengthened to give leadership a high degree of confidence that this primary cause does not emerge to create issues elsewhere. For example, all security testing reports should be provided to an appropriate management level, follow-up activities and resolutions should be formally described and agreed, and strong information security expertise should be applied to understanding the implications of findings and any residual risks.
The risk management processes did not effectively escalate security exposures to management, nor ensure appropriate mitigating actions were taken.	From what we have observed, **the policies and processes at the time did not explicitly require all security risk exposures to be escalated to management. Consequently, this led to this primary cause being evident across the Ministry.** Recently, the Ministry has taken steps to ensure that the governance bodies of projects receive full project risk registers, which, combined with the strongly positive culture towards information security, and the heightened awareness of information security risks, we expect to satisfactorily mitigate this weakness. In addition, greater structure and discipline needs to be applied to information security risk management to give leadership confidence that it is appropriate and robust – for example, ensuring that subject matter expertise is applied to information security risk identification as well as information security risk management, and that information security risks across the organisation have a clear escalation path.

In summary, two of the three primary causes that led to the "kiosk" security breach in October 2012 were not found to be evident across the Ministry, whilst the third primary cause was found to be

evident across the Ministry. A number of actions have been identified by the Ministry and as a result of this review that would strengthen the Ministry's information security approach.

Taking a broader perspective, are there other weaknesses in the Ministry's approach to security that pose risk?

There are other weaknesses in the Ministry's approach to security that pose risk. In our experience, these weaknesses are not unusual for New Zealand organisations. In isolation, each weakness does not present a high level of risk, and our findings do not suggest that the degree of risk within the Ministry is higher than within many similar organisations.

Based on the work we performed within the scope of our review, we found no evidence to indicate that the weaknesses described above have resulted in breaches of security vulnerabilities within the Ministry. However, we would expect that, as part of implementing the recommendations of this review, the refresh of the Ministry's risk framework currently in progress, and through undertaking the improvements already underway, any potential high-risk vulnerabilities would be addressed. Furthermore, the Ministry is committed to working through the process in full for the GCIO Review of Publicly Accessible Systems.

Taking a sound approach to information security and information privacy requires finding an appropriate balance – involving a series of decisions and trade-offs to enable the balance of absolute priorities such as the protection of client personal information, effective and undisrupted service delivery, delivery of a significant programme of legislative driven change, and at reasonable cost.

Hence, because of the importance of the services the Ministry operates and the ever increasing demands it faces - including the push for increased online services and "self-service" delivery, the current level of information security management needs to be improved to better serve the Ministry's current and evolving needs. Also, this will be integral in restoring trust and confidence with the Ministry's clients, the public and external stakeholders.

While a lot of the right building blocks to manage information security are in place, these need to be formalised, led at a senior level, and expanded.

The Ministry has made significant progress to strengthen its approach to information security and information privacy in recent years. This has established many of the building blocks that are needed to manage information security risk effectively.

In addition, the Ministry has a strong culture that clearly understands the importance of privacy and security. This culture has meant that good judgment has generally been applied, even in the absence of more formal structures. The Ministry has also demonstrated a positive willingness to learn the lessons of the October security breach. The Ministry's programme of work to improve its information security approach post October, has further demonstrated commitment to restoring confidence and trust.

However, more needs to be done to achieve and maintain an appropriate approach. While information security is considered in many parts of the organisation, approaches and tools are often informal or lack specificity. This places too much reliance on the capabilities of individual people.

Governance and organisational structures	Leadership and accountability for information security needs to be formally assigned to a senior level within the Ministry, and the organisational structures need to be aligned under that leadership so that responsibilities are clear and activities are prioritised, well-managed and coordinated.
Frameworks and approaches	Strategy, business plans, policies and approaches need to be enhanced and linked so that they are comprehensive in coverage, consistent and sufficiently detailed to support decision making. This needs to include clear definitions of what 'success looks like' for information security, supported by appropriate metrics and targets.
Execution and assurance	Existing processes for information security need to be enhanced and redesigned to ensure that the appropriate activities are carried out. This needs to include implementation of appropriate independent assurance to monitor general business compliance with information security requirements, and to provide confidence that information security activities and controls are adhered to and effective.

Next steps

The Ministry is currently participating in the GCIO Review of Publicly Accessible Systems, which will make public sector wide recommendations on improvements to the security of publicly accessible systems.

The Ministry should continue the information security improvements that are already underway, and consider and implement the detailed recommendations of these reviews.

We expect that by formally assigning information security management to the appropriate senior level within the Ministry, appropriate implementation of the recommendations of this review, and working through the full process of the GCIO review, the Ministry will have confidence in its approach to information security.

Appendix A: Terms of Reference

TERMS OF REFERENCE

Independent Review of the Ministry of Social Development's Information Systems Security

17 October 2012

The Chief Executive of the Ministry of Social Development (the Chief Executive) has commissioned an independent investigation into the security breach that occurred through the Ministry's self-service "kiosks" at two Work and Income service centres, which compromised privacy.

The review will be carried out by Deloitte and will be led by Murray Jack, Chairman, Deloitte (the Independent Reviewer).

A Steering Group, with external stakeholders, including the Office of the Privacy Commissioner and Office of the Government Chief Information Officer, has been set up to provide independent oversight of the review.

This review will take into account the recently announced review of publicly accessible systems by the Government Chief Information Officer.

Objectives of the review

The objectives of the independent review are to address the questions raised about the security of the Work and Income self-service "kiosks" focusing on what happened, why it happened, the lessons learned, and the actions the Ministry needs to take to address any security issues raised.

The review will also assess the Ministry's wider information systems security including the policies, governance and culture, and will make recommendations about the actions needed to be taken to restore and increase public confidence in the Ministry's information systems security.

The review will happen in two phases.

Phase One – Matters in scope

The first part of the review will investigate the circumstances and causes of the "kiosk" security breach which compromised privacy, focusing on

- The establishment and operation of the self-service "kiosks" in Work and Income service centres, including:
    - The work done to ensure appropriate information security was put in place at the time that the "kiosk" infrastructure and services were designed and built;
    - The independent testing done to ensure the security was operating as designed; and
    - The Ministry's response to any security issues identified during the testing.

- Information provided to the Ministry by third parties raising security concerns about the "kiosks" and the appropriateness and effectiveness of the Ministry's response to these concerns.
- The appropriateness and effectiveness of the Ministry's response to the security breach.

Phase Two – Matters in scope

The second part of the review will assess the appropriateness and effectiveness of the Ministry's wider information systems security, particularly publicly accessible systems, and including the policies, governance, capability and culture.

The review will identify any lessons learned and make recommendations to the Chief Executive about any changes and improvements needed to the Ministry's information systems security.

Timeframes and reporting

Phase One - The objective is that Phase One of the review will be completed within two weeks.

Phase Two - The timeframe for the completion of Phase Two of the review will be determined following completion of Phase One.

The reports on both phases of the review will be made publicly available.

Governance

The role of the Steering Group is to provide independent oversight of the review and advice to the Chief Executive.

The Steering Group will consist of external stakeholders[3]. The members are:

- James Ogden – Independent Chair
- Erik Koed – Assistant Commissioner, State Services Commission
- Stuart Wakefield – Director, Office of the Government Chief Information Officer
- Katrine Evans, Assistant Privacy Commissioner (Observer)

In addition, the following people will attend and participate in the Steering Group.

- Murray Jack – Independent Reviewer
- Brendan Boyle – Chief Executive

[3] We note the following changes to the Steering Group for the Phase 2 review:
John Shewan – new Independent Chair, and Mike Flahive, attending for Katrine Evans.

Appendix B: Approach and work performed

Interviews to understand the Ministry's information security approach and practices across both business as usual operations and projects

Around 60 people participated in interviews for this phase of the review. This included the following groups:

- Members of the leadership team
- Members of the Ministry's major service lines
- Governance group members
- Members of the support functions (legal, procurement, human resources, information services, property services, communications, risk and assurance)
- Project team members (roles covered include programme manager, project manager, business owner, business sponsor, business analyst, architect, team lead, testing)
- Physical and information security management and staff
- Members from Information Technology (management and staff covering the areas of application support and development, client services, project management office and infrastructure services)
- An external advisor who has worked with the Ministry's IT team and members of the leadership team

Reviewing projects to understand the security practices undertaken

We selected three projects to understand the Ministry's information security approach towards projects. The sample was selected from a candidate list with the criteria that the duration is greater than 3 months, is a representation of initiatives involving the major service lines, includes some form of external interaction, and initiation was within the last two years. Selected projects were business initiatives with a significant IT component. Key features of the three projects are:

- **Project one** – A large programme of work initiated due to changes in legislation. It consists of multiple subsidiary projects and multiple phases. The programme is still in progress.
- **Project two** – A project that involved working with another agency for data sharing. This project was in progress for some of the similar time period as the "kiosk" project and has been completed.
- **Project three** – A project that involves development and implementation of a web application. This project is still in progress.

Reviewing documentation

We have reviewed nearly 700 documents over the course of this phase of the review. This includes the following types of documentation:

- Security strategy documents
- Policy and processes documents
- Project documentation including methodology and specific artefacts from the projects. For example:
    - Project initiation documentation
    - Solution architecture design documentation
    - Meeting minutes
    - Security testing results
    - Risk registers
    - Test plans
- Concept papers
- Business as usual operations risk registers
- Human resources documentation
- Governance charters
- Responses to external reviews
- Test results for security testing conducted as part of business as usual operations
- Network diagrams and sample of technical documents
- Vendor contracts
- Legal documents
- Memoranda

Undertaking a survey and holding focus groups to provide insight to the Ministry's culture towards security

We reviewed engagement and risk survey methods, and the resulting insights from previous culture surveys conducted by the Ministry.

We developed an information security culture survey to understand the Ministry's attitude to and understanding of information security. A sample of 135 individuals from across the Ministry (including front line and back office staff) was selected. 105 responses were received. This survey was not intended to provide a statistically significant, quantified analysis of the Ministry's culture towards information security. Rather, it was to provide us with a broad view of what the people within a cross-section of the Ministry felt and thought about the topic.

We also held five focus groups to further assess the attitude to and understanding of information security at the Ministry. Representatives from the following areas were included in the focus groups:

- Software developers
- Business support functions
- Front line of the major service lines
- Cross section of IT
- Project team members from a variety projects

Appendix C: Security improvements underway

Since the "kiosk" breach in October 2012, the Ministry has commenced a programme of work to improve its information security approach. The Ministry has shared the following status with us on the programme activities underway. We understand that these activities may be subject to change based on the recommendations in this report.

Completed

Governance
- Creation of a programme for information security
- Work on an initial security governance framework
- Strengthen IT management group to provide additional oversight

Policies and Processes
- Work on a centralised security vulnerabilities repository
- Work on an external applications inventory

In Progress

Governance
- Review of existing governance structure

Policies and Processes
- Review and update of IT project management processes and templates
- Review and update information processes and templates
- Establish additional formal information security standards
- Improve security monitoring across infrastructure and applications
- Internal review of patching of Ministry systems
- Internal review of firewall rules
- Strengthening application security
- Penetration testing of external facing applications
- Internal review of access controls

Capability
- Improve information security knowledge and testing capabilities within the Ministry

Culture
- Work on a coordinated education programme for information security risks, policies and expectations

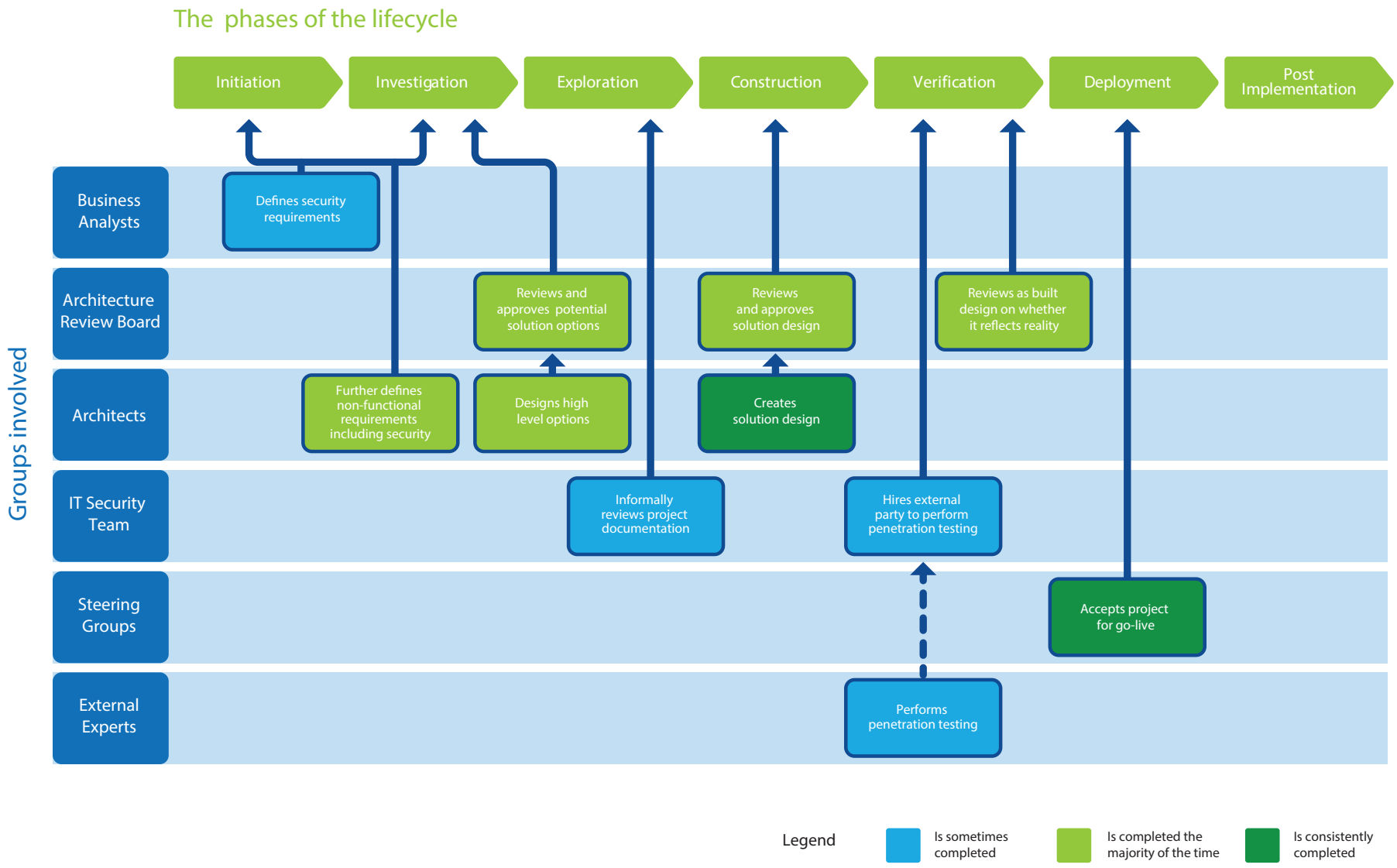
Planned

Policies and Processes
- Review of infrastructure architecture
- Improve intrusion prevention / detection systems
- Internal review of external facing applications against good practice web application standards

Security Risk Management
- Capture past and current security risk decisions

Appendix D: Security input during projects

For projects that have IT components and that the Ministry categorises as significant, a standardised seven step methodology is used. Within the methodology, there are various formal and informal security touch-points which are mapped below. We found variances between when and if these touch points occur within processes.



Appendix E: Culture responses

Information Security Culture

To obtain an understanding of what people from a cross section of the Ministry felt and thought about information security and information privacy, we:

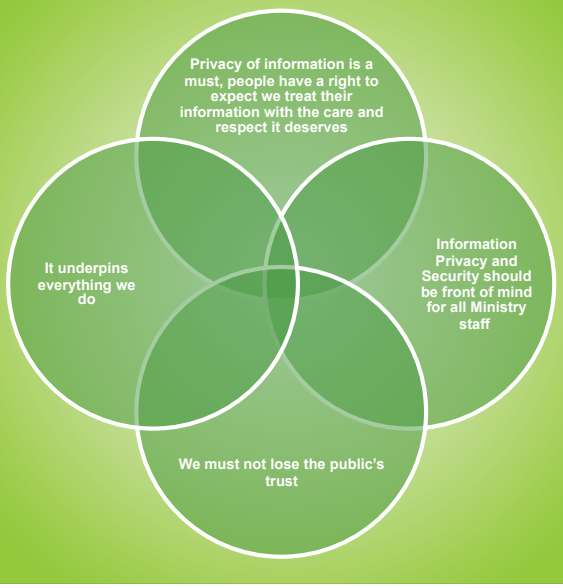
- Selected a sample of 135 individuals from across the Ministry (including front-line and back office staff) to complete an information security culture survey. 105 responses were received.
- Reviewed various internal engagement and risk surveys carried out previously by the Ministry.
- Held five focus groups to further assess the attitude to and understanding of information security and information privacy across a cross section of individuals including representatives from project teams, business support functions, front line of the major service lines, and a cross section of IT
- Asked questions on culture of the Ministry as part of wider interviews conducted through this review.

Based on the culture survey

The top three most cited statements
(strong agreement expressed)

Based on the culture survey, focus groups and interviews

Key attitudes towards information security and information privacy



Appendix F: Glossary

Term	Explanation
ARB (Architecture Review Board)	The Architecture Review Board is a technical body within the Ministry that is used to review solution designs when major IT changes or development occurs. The Architecture Review Board checks that the designs align with the directions set by the Ministry's enterprise architecture. Membership of the Architecture Review Board includes Enterprise Architects and representatives from Infrastructure and Services.
Business as Usual (BAU)	The Ministry's normal execution of its standard operations. Projects and programmes are transitioned to business as usual after they have completed or implemented the changes they were tasked with introducing.
BSG (Business Steering Group)	The Business Steering Group is a governance body set up when projects are established within the Ministry. The business steering group provides the project with overall direction, guidance and support, and monitors the project to facilitate successful implementation. Membership of the Business Steering Group typically includes representation from the business area, the business owner, risk and assurance, and information technology.
Business Case	A document detailing the reasons or need to initiate a project as well as proposed solution designs and funding requirements.
Code of Conduct	The set of guidelines outlining the ethical responsibilities and actions of Ministry employees and contractors.

Term	Explanation
Deputy Chief Executive (DCE)	A senior member of the Ministry's leadership team who reports directly to the Chief Executive.
Enterprise architects	Enterprise architects work with business stakeholders, to build an overall view of the Ministry's IT strategy, processes, data, and assets. The enterprise architects use this view to suggest project options that are in alignment with the Ministry's IT strategy to solution architects.
GCIO (Government Chief Information Officer)	The Government Chief Information Officer (GCIO) has the mandate from the government to provide leadership in information and communications technology (ICT) to drive performance improvement across the system. The Government Chief Information Officer resides within the Department of Internal Affairs.
Governance	Governance relates to consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility.
Information Management Strategy	A strategy document that sets out standards, approaches and guidelines for • How information is managed and maintained end-to-end, i.e. including information capture through to information archiving and disposal. • How information is classified • How information is used • The value of information
Information Privacy	The set of actions and decisions an agency makes on how it uses, handles and looks after personal information given to them.
Information Security	Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, recording or destruction.

Term	Explanation
"Kiosks"	"Kiosks" refers to the computers, and the associated stands and devices (e.g. keyboards) provided at Work and Income offices for self-service to enable job seekers to create CVs, search and apply online for jobs.
IT PMO (IT Project Management Office)	The IT PMO is responsible for supporting and maintaining the Ministry's IT project methodology to be used by projects.
IT Work Management	The Ministry's project management methodology used to guide the Ministry's business and IT staff. It contains process steps and templates for engaging Information Technology to do new work or progress existing work.
Legal Services	A group within the Ministry that provides a variety of legal support to the Ministry including reviewing contracts with suppliers and other government agencies to ensure that appropriate privacy and security requirements are in place.
New Zealand Information Security Manual (NZISM)	Document produced by the Government Communications Security Bureau to provide technical policy advice and requirements to assist government departments and agencies in securing information systems and the data stored in those systems. The latest version was released in June 2011. http://www.gcsb.govt.nz/newsroom/nzism.html
New Zealand Security in the Government Sector	Manual issued by the Interdepartmental Committee on Security which sets out protective security policies, principles and procedures. Additional guidance and more detail are provided in the NZISM. Together they provide updated guidance on securing government functions, resources and information from any sources of harm. http://www.nzsis.govt.nz/publications/security-in-the-government-sector.html
Penetration Testing	Security testing of a system or network by replicating the types of actions a malicious attacker would conduct.
Procurement	A group within the Ministry that provides advice to other areas of the Ministry around contracts with suppliers and purchasing of third party services.

Term	Explanation
Risk and Assurance	A group within the Ministry that plays a key role in ensuring the Ministry applies a methodological and effective framework for managing risk, is operating within its governing rules and regulations, and that operational management practices are effective and efficient.
Risk Register	A documented list of risks identified by a project or organisation. It typically acts as a central location of identified risks to be monitored and tracked to assist with managing identified risks before become problems. A risk register details information about the risk, how likely it is to occur, the impact if the risk occurs, what controls if any are in place to remediate the risk, and individual or role responsible for monitoring the risk and keeping the risk register updated in relation to the latest information about the risk.
ROI (Return on Investment)	A financial calculation to determine the financial and non-financial benefits of a specific investment.
Solution Architects	Project member who designs the high-level design solution and dictates low-level technical standards, including software coding languages, application and hardware platforms and communication interfaces.
SLAs (Service-level agreements)	A service-level agreement is typically a formal agreement on the level of service that IT or a third party will provide to the business for a system.
Workplace Services	Workplaces Services is the name of a group within the Ministry that is responsible for property management and physical security of the Ministry.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/nz/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 170,000 professionals are committed to becoming the standard of excellence.

Deloitte New Zealand brings together more than 900 specialists providing audit, tax, technology and systems, strategy and performance improvement, risk management, corporate finance, business recovery, forensic and accounting services. Our people are based in Auckland, Hamilton, Wellington, Christchurch and Dunedin, serving clients that range from New Zealand's largest companies and public sector organisations to smaller businesses with ambition to grow. For more information about Deloitte in New Zealand, look to our website www.deloitte.co.nz