KPMG

cutting through complexity

GCIO Review of Publicly Accessible Systems

Summary of Findings

December 2012

Disclaimers

Inherent Limitations

This report has been prepared as outlined in the Scope and Approach section of this report. The procedures outlined in the Scope and Approach section constitute neither an audit nor a comprehensive review of operations. The findings in this report are based on a qualitative study and the reported results reflect a perception of the State Sector but only to the extent of the sample surveyed, being the Department of Internal Affairs (DIA) approved representative sample of systems. Any projection to the wider IT environment is subject to the level of bias in the method of sample selection. No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, State Sector staff and contractors consulted as part of the process. We have not sought to independently verify those sources unless otherwise noted within the report. In the course of undertaking this review KPMG has identified potential conflicts of interest to DIA and agreed processes for managing them

Any reference to 'review' throughout this report has not been used in the context of a review in accordance with assurance and other standards issued by the New Zealand Institute of Chartered Accountants.

KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form. The findings in this report have been formed on the above basis.

Due to the inherent limitations of any internal control structure it is possible that errors or irregularities may occur and not be detected. Our procedures were not designed to detect all weaknesses in control procedures as they are not performed continuously throughout the period and the tests performed are on a sample basis. As such, except to the extent of sample testing performed, it is not possible to express an opinion on the effectiveness of the internal control structure.

Third Party Reliance

This report is solely for the purpose set out in the Scope and Approach section of this report and for the Department of Internal Affair's information, and is not to be used for any other purpose or distributed to any other party without KPMG's prior written consent. This report has been prepared at the request of the Department of Internal Affairs in accordance with the terms of the contract between KPMG and DIA. Other than our responsibility to the Department of Internal Affairs, neither KPMG nor any member or employee of KPMG 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.

Contents

Glossary

CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology - a framework created by ISACA (www.isaca.org) for information technology management and governance
Control (noun)	In the context of this report means a mitigation
(the) Department	The Department of Internal Affairs
DIA	Department of Internal Affairs
DSO	Departmental Security Officer
GCIO	Government Chief Information Officer - the GCIO is also the Chief Executive of the Department of Internal Affairs
Information security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction
IT	Information technology
ITSM	IT Security Manager
MSD	The Ministry of Social Development
NZISM	New Zealand Information Security Manual
PIA	Privacy Impact Assessment
Publicly accessible system	A system as defined in Section 3.1 of this report
Sector	In the context of this report means the State Sector
SIGS	Security in the Government Sector standard
System	In the context of this report means a publicly accessible system, as further defined in this report
WINZ	Work and Income New Zealand, a business group within the Ministry of Social Development

1 Executive summary

On 14 October 2012, freelance journalist Keith Ng alerted on his blog that he was able to access sensitive personal information via two kiosks within a branch of Work and Income New Zealand (WINZ), a business group within the Ministry of Social Development. He asserted that these files included invoices detailing the medical conditions of vulnerable children in State care.

Following the WINZ kiosk security breach, the State Services Commissioner and Head of State Services tasked the Government Chief Information Officer (GCIO) to undertake an urgent review of publicly-accessible systems operated by the State Service. A Terms of Reference was released on 19 October 2012 and KPMG was appointed to assist the GCIO in responding to the Terms of Reference. This report sets out KPMG's summary of findings resulting from its assessment of the security and privacy practices within the State Sector as it relates to the GCIO's Terms of Reference. The Terms of Reference also required KPMG to review the independent reports commissioned by the Ministry of Social Development in response to the kiosk security breach.

As part of the Better Public Services programme there will be more government services delivered via digital channels. Consequently it will become increasingly important that users of government services can have trust and confidence in the sector's appropriate use and protection of their personal information via this channel.

Our assessment consisted of a review of agency provided documentation to help inform us about the security and privacy risk identification processes agencies undertook in the design of their publicly accessible systems, the controls (mitigations) they designed in response to those risks, and the assurance they sought over the appropriateness and effectiveness of those controls. Additionally, we sought to identify whether, more generally, appropriate governance structures such as roles, policies, standards and procedures were in place to manage security issues.

It is worth noting that there are some inherent limitations with a document based review such as this. We have not, for example, been able to test whether controls have been effective in mitigating the risks identified unless agencies have commissioned such an assessment themselves. Nor have we been able to assess non-documented controls or understand whether the absence of controls relates to an explicit decision.

Notwithstanding these limitations, some clear patterns have emerged and the summary is that the level of security management maturity across the state sector is lower than could reasonably be expected to provide the public with appropriate assurance about the safety of their private information. Whilst examples of good practice exist, many agencies lack fundamental components of good security and privacy practice such as comprehensive security policies, security risk management frameworks and the gaining of assurance over their practices or the security controls implemented within the systems. Such practices will never avoid failure altogether - their purpose is more to ensure that risks are managed according to the risk appetite of the organisation. We set out our findings in more detail in Section 4 and provide advice to agencies in Section 6.

Our review did not discover any loss of private data or similar breaches. We did identify 13 agencies with potentially high priority unresolved vulnerabilities, and these were escalated to the Department of Internal Affairs for further action as we progressed through our documentation review. A further five agencies were identified; however we understand that three agencies had actually resolved the vulnerabilities prior to this review, and that the remaining two agencies already had actions underway at the time of the review. We provide a summary of the vulnerabilities present for these 13 agencies in Appendix III.

Although the independent reports commissioned by the Ministry of Social Development were more specific than this review, our view is that there are strong similarities between the findings of the different reviews.

2 Background and context

Part of the Better Public Services programme includes the delivery of more government services via digital channels[1]. As the sector does so, it will become increasingly important that users of government services can have trust and confidence in the sector's appropriate use and protection of their personal information via these channels. Furthermore, the trajectory of more joined up services to citizens and businesses means that trust and confidence in the sector will only be as strong as the weakest link.

In summary, more services are being added to digital channels and the services will be more connected. Regardless of the current state of practice, the inherent risk profile associated with publicly accessible systems, and the expectations of the public, are only likely to increase over time. There is a need for the sector to keep pace with these expectations.

On 14 October 2012, freelance journalist Keith Ng alerted on his blog that he was able to access sensitive personal information from two kiosks available within a Work and Income New Zealand (WINZ) branch[2]. He asserted that these files included invoices detailing the medical conditions of vulnerable children in state care.

Privacy issues and privacy breaches have also been topical in the media over the last several months[3], and a recent One News Colmar Brunton Poll[4], issued on 31 October 2012, stated that 60% of respondents did not trust government departments to protect their personal details.

Following the WINZ kiosk security breach, the State Services Commissioner and Head of State Services, Iain Rennie, tasked the GCIO, Colin McDonald, to undertake an urgent review of publicly-accessible systems operated by State Services[5]. This occurred on the 16 October 2012. A Terms of Reference was released on 19 October 2012 and KPMG was appointed to assist the GCIO in responding to the Terms of Reference[6].

This report sets out KPMG's summary of findings resulting from its assessment of the security and privacy practices within the state sector as it relates to the GCIO's Terms of Reference.

[1] Source: SSC Better Public Services: Improving Interaction with Government: http://www.ssc.govt.nz/bps-interaction-with-govt

[2] Source: MSD's leaky servers from http://publicaddress.net/onpoint/

[3] Source: Immigration staff axed over privacy breaches: http://www.stuff.co.nz/national/politics/7981525/Immigration-staff-axed-over-privacy-breaches

[4] Source: One News Colmar Brunton Poll 27-31 October 2012: http://www.colmarbrunton.co.nz/images/ONE_News_Colmar_Brunton_Poll_report_27-31_Oct_2012_NEW.pdf

[5] Source: Head of State Services tasks GCIO on privacy review from http://www.ssc.govt.nz/head-state-services-tasks-gcio-privacy-review.

[6] Source: Terms of Reference released for privacy review from http://www.dia.govt.nz/press.nsf/d77da9b523f12931cc256ac5000d19b6/8c617fb1f262abe5cc257a9c000abe38!OpenDocument. The Terms of Reference are also attached as Appendix I.

3 Scope and approach

3.1 Scope

The scope of the review included 70 State Sector agencies, with a total of 215 publicly accessible systems between them: 141 Internet, 38 kiosk and 36 wireless networks. The in-scope agencies are set out in Appendix II.

Publicly accessible systems included any IT system where there was the potential for unauthorised access to personal information by members of the public, as part of their normal interaction with an agency via their IT system. In the context of this report, "public" includes individuals, corporate entities or similar organisations.

Within the above context, the in-scope systems included:

- **Kiosks** – any computer connected to an agency network that members of the public have access to. Examples include:
  - Visitor sign in systems, usually found at reception desks
  - Computers provided to access Internet based systems from within agency premises
  - Computers provided to access internal services from within agency premises.
- **Transactional based Internet systems** – any Internet based services provided to the public which allow the public to transact or access information that is sensitive or confidential to members of the public, or to the agency. Examples include:
  - Websites used to access sensitive or private records held by any agency
  - Websites used to provide sensitive or confidential information to an agency.
- **Wireless networks** – any wireless network where temporary or guest access is provided to members of the public.

3.2 Scope exclusions

The scope of the review did not include:

- Technical testing of the operating effectiveness of the security
- An assessment of whether controls has actually been implemented within a system (the review relied upon agency provided documentation)
- An assessment of any systems or networks intended only for the use of agency employees or contractors, other State Sector employees or contractors, or for communications between agencies – this includes such aspects as reception computers and network access points that may be located in publicly accessible areas within an agency's premises
- Any publicly accessible telephone system within an agency's premises
- Any Internet systems or wireless networks beyond those described in the scope above, such as Internet systems that provide access to public registers of information
- An assessment of the broader security related risks posed by systems, beyond the risks to the confidentiality of sensitive or confidential information held by agencies.

3.3 Approach

The security applied over the publicly accessible systems, and the wider security practices used by agencies, was assessed by performing a desk based review of documentation provided by the in-scope agencies. In addition, we reviewed the independent reports commissioned by the Ministry of Social Development (MSD) in response to the kiosk security breach.

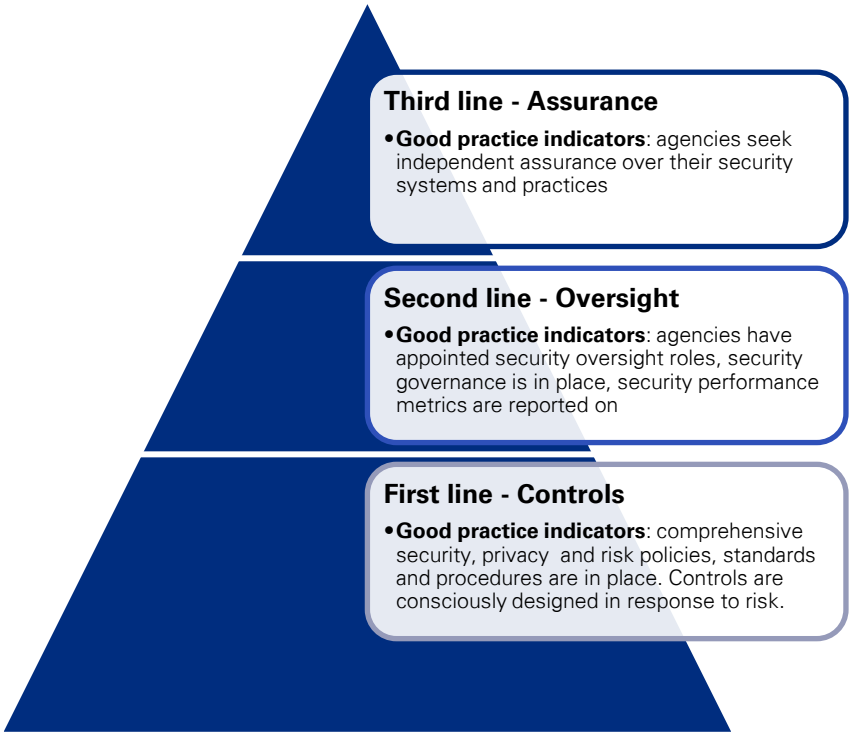


Figure 1: The "three lines of defence" risk management model. The first line of defence is an appropriate controls environment - policies, standards and procedures - that is utilised by operational management. The second line of defence is oversight of the controls through use of risk management, compliance or performance management functions. The third line of defence is assurance of the controls via a (semi) independent entity such as internal audit or an external provider.

Our assessment was aligned with the "three lines of defence" model commonly used for risk management[7] (see Figure 1).

The **first line of defence** relates to activities carried out in the operational management of the organisation. These are defined by policies, standards, procedures and frameworks and designed to mitigate and manage risk. In security and risk management parlance, the mitigations are called "controls". Good practice indicators of appropriate security and privacy controls would include: evidence of comprehensive security and privacy policies and procedures, certification/accreditation frameworks to accredit systems for operational deployment, clear and documented security accountabilities and roles, and formal security risk management processes.

The **second line of defence** relates to oversight functions. Good practice indicators include: the appointment of security oversight roles and governance forums, security and risk management reporting requirements and performance metrics, and appropriate escalation processes.

[7] A more detailed description can be found here: https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Global%20Advocacy%20Platform.pdf

The **third line of defence** relates to (semi) independent[8] assurance. Indicators of good practice would include independent and internal audit security reviews and/or compliance reports on system security and security practices within the agency.

The information used for the desktop review was gained via an information request to agencies. The responses were then analysed and subsequently validated with agencies. The analysis was then used to produce findings, and combined with the findings from MSD's independent reviews, used to inform the advice to agencies in Section 6 of this report.

3.4 Inherent limitations

Given the nature of the desk based review, there were some inherent limitations. The review has not tested the design and operating effectiveness of the controls in place. This means that, where there was evidence of controls being designed, we have not been able to assess whether they have been implemented or whether they are effective, unless the agency has undertaken or commissioned an assessment themselves. Sometimes controls and practices exist in un-documented form. Given that the review has relied on agency provided documentation, we have not been able to assess whether such un-documented controls exist within agencies.

Additionally, where controls were absent, we have not been able to determine the reason why this might be so.

3.5 Governance

An advisory group supported and advised the GCIO on the findings and resulting recommendations of the review. The group consisted of the GCIO as Chair, and members from the Department of the Prime Minister and Cabinet (DPMC), the Government Communications Security Bureau (GCSB) and the State Services Commission (SSC). An observer from the Office of the Privacy Commissioner (OPC) also attended. The Terms of Reference is set out in Appendix IV of this document.

[8] Semi-independent assurance would include assurance provided by an internal audit function, for example, versus fully independent assurance provided by a third party.

4 Findings

This section sets out the findings resulting from the analysis of KPMG's review. Whilst examples of good practice exist, many agencies lack fundamental components of good security and privacy practice such as comprehensive security policies, security risk management frameworks or the gaining of assurance over their practices or the security controls implemented within the systems.

4.1 There are examples of good practice within the sector

A number of agencies have been able to demonstrate good practice in a number of areas. That is, they have been able to show:

- There is an appropriate controls environment, with documented policies, standards and procedures in place, and in the case of systems, appropriate risk assessment and controls design
- There is appropriate oversight of the controls, such as specific roles and accountabilities, and governance structures
- There is an appropriate level of assurance over their controls.

We discuss elements of good practice in Section 6 of this document.

4.2 A small number of unresolved high priority issues have been identified and escalated for agencies to take immediate action

It is good practice to seek assurance over different security controls implemented to ensure that the controls are appropriate and effective. It is equally important to act[9] on the recommendations that result from assurance activities.

We reviewed assurance documentation provided by agencies relating to their publicly accessible systems, and identified 13 agencies with potentially high priority vulnerabilities that did not appear to have been resolved at the time of our initial review. These issues are summarised in Appendix III.

It is important to understand that these issues were identified as high priority from assurance documentation provided by agencies. As we state further below, many agencies were unable to provide us with such documentation, and therefore we are unable to comment in such cases whether further high risk issues exist.

4.3 Most agencies have security policies in place, but many are not supported by standards and procedures

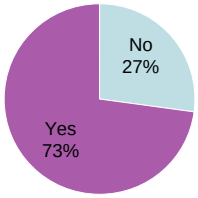
Good security policies and standards are a cornerstone to good security practice and are a fundamental "first line of defence" control. Policies cannot stand alone – they should link to detailed security standards which translate the objectives outlined in security policies into functional policies that provide the foundation for the configuration and management of security. A more detailed description of policies, standards and procedures can be found in Section 6.6.

We reviewed whether agencies had a formal security policy. Evidence of such a policy would indicate that a foundational element of security practice was in place. We then assessed whether the policy was supported by standards and procedures. This would indicate that the policy can be applied consistently, whereas absence of such standards and policies would indicate that application of policy could be difficult or inconsistent. Finally, we also assessed whether formal security certification and accreditation

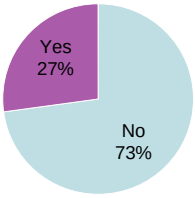
[9] Remediation of issues raised is the most obvious response, but formal risk acceptance is also an appropriate response. It remains a question for the Head of State Services to contemplate the degree of risk a Chief Executive should tolerate given the wider risk borne by the sector when issues arise.

processes were in place. The existence of such processes would indicate that the agency has a structured approach to assessing the security of its systems prior to commissioning. Absence of such processes could indicate that the agency had an ad-hoc approach to assessing security prior to commissioning, which could yield inconsistent results and unknowingly introduce risk.

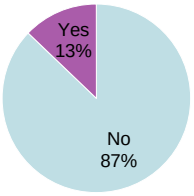
Possess a formal security policy



Comprehensive security policies and procedures are in place



Formal security certification and accreditation processes exists



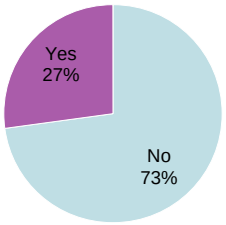
Most agencies (73%) possess a formal security policy. Many agencies (73%), however, lacked formal security standards and procedures to enable the policies. A high number (87%) also did not have formal security certification and accreditation processes to assess their systems.

4.4 Most agencies lack formal robust security risk management processes

As another first line of defence mechanism, good risk management practices are the fundamental driver of appropriate security and privacy measures. Security and privacy risk management should link upwards into a wider enterprise risk management framework and downwards into security design practices, security controls, standards and processes.

We reviewed documentation for evidence of formal security risk management processes. Evidence of such documentation would indicate that security risks were being appropriately and consistently assessed and linked into the wider enterprise risk management framework. Absence of such processes could indicate that security risks are not being assessed and managed (ie. responded to), or that it is being done in an inconsistent manner that is isolated from the wider enterprise risk management framework.

Formal security risk management processes are in place

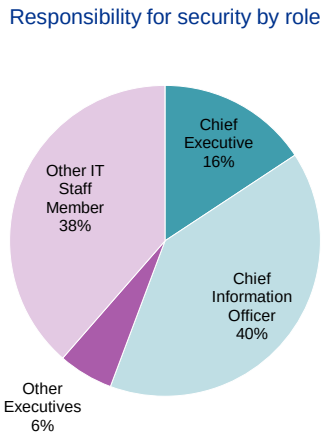


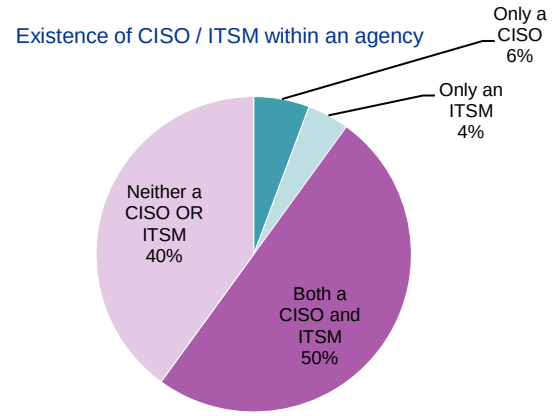
We have found that many agencies (73%) do not have formal security risk management processes. This is a significant issue as it is fundamental to driving appropriate response such as design of controls or testing.

4.5 Responsibility for security varies across the sector

One important control for the management of security and privacy is the allocation of roles and accountabilities in an organisation. This should also include oversight accountabilities – a second line of defence mechanism. Ultimately the Chief Executive is responsible, however it is usual practice to assign supporting roles such as a Chief Information Security Officer (CISO) and an IT Security Manager (ITSM). A CISO is responsible for setting the strategic direction for information security within an organisation whereas an ITSM translates the directives into technical activities for the IT organisation to implement.

Agencies identified who in their organisation is responsible for security, within their response to the information request. Given the nature of the question, some caution is required in interpreting the response. However, a response identifying an executive level responsibility could indicate a reasonable level of oversight and accountability for security matters. Absence of executive responsibility could indicate that that security matters do not get sufficient executive visibility and that security matters are isolated from wider business matters. We also reviewed whether a CISO and ITSM were identified within the agency. Presence of such roles is an indicator of good accountability and governance to manage information security matters. Absence may indicate that such accountabilities may not exist, although it is possible that such accountabilities exist within other role definitions.





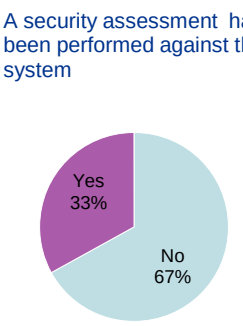
In 38% of cases, agencies identified someone other than a senior executive as being accountable for security. Half of the agencies had both a CISO and ITSM appointed, and 40% had neither.

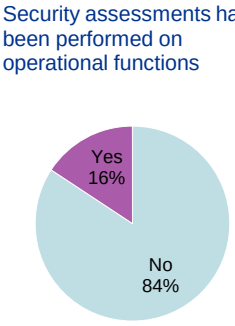
4.6 There is limited evidence that agencies are seeking assurance over their publicly accessible systems or security management processes

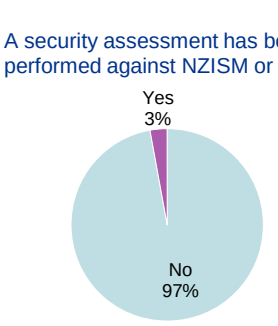
As mentioned above, it is good practice to seek assurance over different controls that agencies may be using to ensure that controls are appropriate and effective. This is a fundamental "third line of defence" activity. Assurance activity should cover security management controls (such as security risk management policies and processes) and system specific security controls (such as password management controls), and also span the full lifecycle of a system. In the case of specific systems, this means seeking assurance over the security/privacy design elements and testing whether or not the controls have been implemented and are effective.

We reviewed whether agencies had performed an assessment of their compliance with government security standards[10], or whether they had assessed the security of their systems or their security management practices. Presence of such assessments would indicate that the agency was engaging the third line of defence (assurance) appropriately, while absence would indicate an over-reliance on control or oversight mechanisms.

[10] The New Zealand Information Security Manual (NZISM) or the Security in Government Sector standard (SIGS)





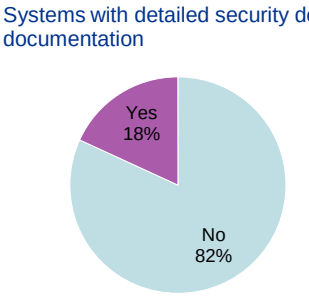


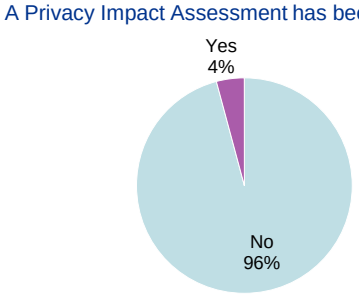
Generally, there is limited evidence of such assurance being sought over standards, processes and systems. Only 3% of agencies have assessed their compliance with SIGS and NZISM, with 16% having sought assurance over key security management functions or processes such as change and incident management. Of the systems in scope, one third had a security assessment performed.

4.7 There is limited evidence that security and privacy controls are being explicitly designed into publicly accessible systems

As privacy and security risks are identified, it is good practice to design appropriate controls to mitigate these risks. This might include, for example, the use of specific encryption techniques or controls to validate the data entered into systems. These are "first line of defence" activities. In a typical system design, this would manifest in a security assessment and explicit consideration of privacy (as evidenced by a privacy impact assessment[11]), and then in requirements documentation to allow for the development of the system.

Documentation was reviewed to determine whether agencies had undertaken detailed formal security designs for their in-scope systems. Where such documentation is available, this would indicate that security risks had been assessed and corresponding controls had been designed to mitigate them. Absence could indicate that security had not been explicitly designed to address the specific risks of the system. Similarly, we reviewed whether agencies had assessed the privacy impact of their systems. As with security risks, this would indicate that privacy had been consciously considered and appropriate controls designed to address potential risks and impacts.





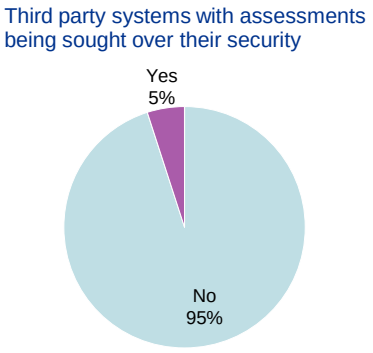
Of the systems evaluated, 82% did not have detailed security design documentation and the overwhelming majority of systems did not have an associated Privacy Impact Assessment. While this does not mean that security and privacy risks have not been considered and that the systems are vulnerable to such risks, there is reliance on a more informal approach to assessing and designing appropriate security and privacy controls.

[11] http://privacy.org.nz/privacy-impact-assessment-handbook/

4.8 Most agencies using third party systems are doing so without assessing the security of those systems

A number of agencies use systems provided by third parties. It is important that any such systems meet appropriate security and privacy standards, and that agencies receive the same level of assurance as they do for their own systems.

Evidence of a security assessment[12] over a third party system would indicate that the agency had formally considered security risks and assessed the security of the third party systems. Absence of a documented assessment could mean that the agency had not adequately considered security risks, or had assessed security in an ad hoc or cursory manner. This could introduce unknown, and therefore uncontrolled, risks to the agency.

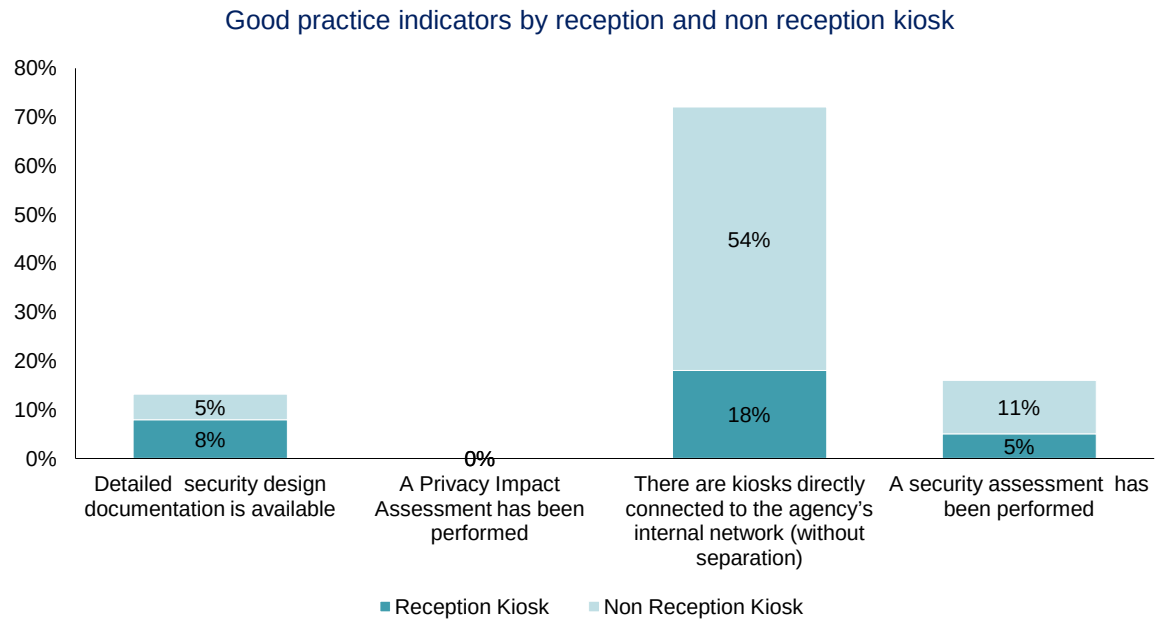


Only 5% of the in-scope third party systems reviewed had undergone a formal security assessment. Agencies are therefore placing reliance on third party providers to have appropriate security controls in place.

4.9 Many kiosk systems have a higher risk of security vulnerabilities than other publicly accessible systems

In the analysis below we have assessed a number of good practice indicators for publicly accessible systems. These include processes for the identification of security and privacy risk, the design of appropriate controls, and assurance over these controls. Given the recent vulnerabilities with the MSD kiosks we have also assessed these systems separately. There were 38 kiosk systems in total, 13 of which were reception visitor sign-in kiosks (i.e. computers typically found in reception areas to provide automated sign-in functionality).

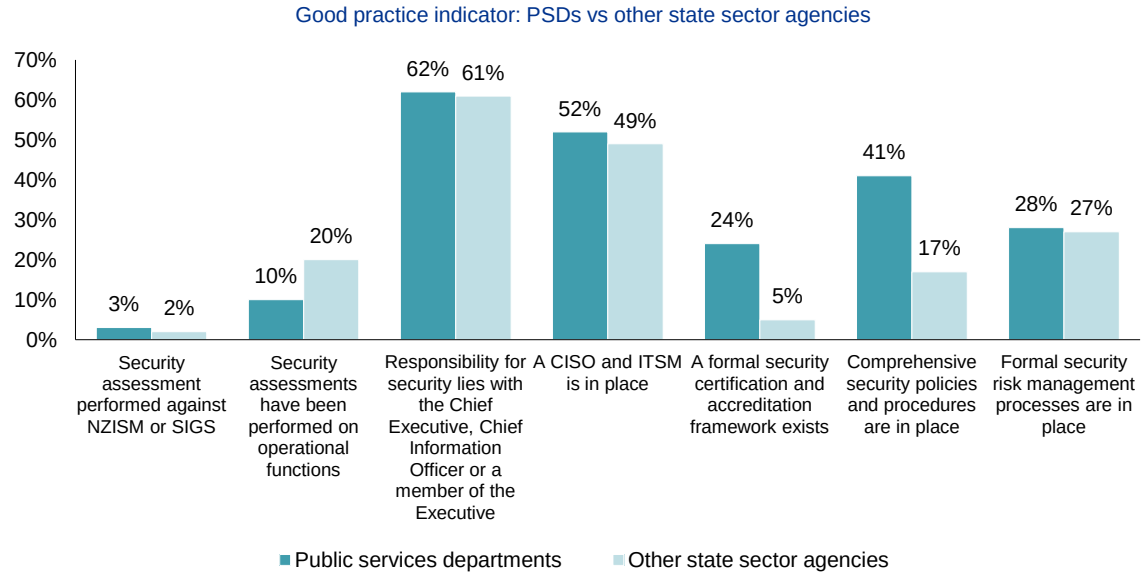
[12] Note we have taken a broad view of what an assessment might entail in this case. It could mean an internal, but formal, review of the security measures undertaken by the third party (second line of defence), or it could be assurance provided by an independent provider (third line of defence).



Of the kiosk systems reviewed, 13% had detailed security design documentation and none had a privacy impact assessment (compared with 18% and 4% respectively for all publicly accessible systems). Almost three-quarters of the kiosk systems were directly connected to the internal networks of agencies without the use of network separation techniques. This increases the risk of unauthorised access to sensitive data. Roughly one quarter of these kiosk systems are used for visitor registration and the opportunity in these cases for individuals to gain unauthorised access is lowered due the location and likelihood of monitoring by reception staff. Only 16% of kiosk systems had a security assessment undertaken compared with 33% overall.

4.10 There are only minor differences between different agency segments

We analysed whether there were significant differences between core public service departments and other entities.



Overall the differences are minor but consistent. Generally speaking, public service departments have slightly more mature practises than other state sector agencies.

5 Lessons learned from the MSD reviews

The Terms of Reference for the GCIO Review of Publicly Accessible Systems required consideration of lessons learned from the MSD kiosk security breach. We summarise the reports below along with brief commentary.

In response to the kiosk privacy breach, the Chief Executive of MSD commissioned Deloitte to conduct two investigations (Phase 1 and 2) to undertake an independent review of information systems security within the Ministry. Phase 1 focussed on issues specifically relating to the kiosk breach, and Phase 2 on wider information systems security (including policies, governance, capability and culture) within the Ministry[13]. Taken together the scope[14] of both reports went both wider and deeper than the scope of this report. We have repeated findings from aspects of both reports that could be considered relevant to this report.

5.1 Phase 1 Report: Circumstances and Causes of, and Response to, the "Kiosk" Security Breach

The Phase 1 Report focussed on the development and operation phases of the MSD Kiosks, as well as the circumstances of the security breach and the Ministry's response. While the management response was found to be well considered and co-ordinated, the report's findings in relation to the development and operation the kiosks are most relevant to this report:

5.1.1 Findings from the development phase

a) There was insufficient focus on security and privacy during design and build

b) There was appropriate testing and advice to ensure security

c) There was an inadequate response to findings from the security testing

d) There was inadequate risk management and escalation within the IT organisation

e) There was incomplete project information and policies.

5.1.2 Findings from the operate phase

a) There was a lack of adequate monitoring

b) There was an insufficient audit trail

c) The policy and process on the level of trust to be assigned to the kiosk device is unclear and inconsistent

d) There was no alerting of suspicious activity Commentary on the Phase 1 Report.

This report focussed on the development and operation of one publicly-facing system – the kiosks. However, the findings are entirely consistent with the analysis of the prior section, which indicate the need for better security risk management, better security and privacy controls design and better integration of privacy and security management within the solution delivery lifecycle (which informs how projects are managed).

5.2 Phase 2 Report: Review of Wider Information Systems Security

The Phase 2 Report was a much wider-ranging review of the Ministry's Information Systems Security. It concluded that two of the primary causes of the kiosk security breach were not widespread across the Ministry. These were the fact that security was not adequately designed into the kiosk project and that

[13] Source: "Independent Review of the Ministry of Social Development's Information Systems Security", 17 October 2012, http://www.msd.govt.nz/about-msd-and-our-work/newsroom/media-releases/2012/independent-review-of-the-ministry-of-social-developments-information-systems-security.html

[14] http://www.msd.govt.nz/documents/about-msd-and-our-work/newsroom/media-releases/2012/independent-review-deloitte.pdf

exposures identified by penetration testing were not appropriately addressed and followed up. However the third primary cause of this breach, that risk management processes did not effectively escalate security exposures and that appropriate action was taken, was evident across the Ministry. The Phase 2 Report made findings in relation to both business as usual and project information systems security.

5.2.1 Business as usual information security review

5.2.1.1 Findings

a) Information security is not explicitly considered within existing governance arrangements
b) The team structures relating to information security do not reflect increasing demands
c) There is no enterprise-wide approach to information security risk management
d) Performance measures and target outcomes for information security are not defined
e) Visibility of information security controls and assurance over the business as usual environment is limited
f) The Ministry has a strong culture that values the importance of privacy and information security
g) Mechanisms to maintain a view of the information security risk profile are not in place
h) Alignment with external requirements
i) Information privacy practices appear to be well defined and consistent.

5.2.1.2 Recommendations

a) Assign Deputy Chief Executive (DCE) level leadership and accountability for information security
b) Integrate information security into strategic planning and performance monitoring
c) Improve information security risk management, control and assurance approach.

5.2.2 Projects information security review

5.2.2.1 Findings

a) Information security governance and responsibility on projects is not well-formed
b) There are insufficient formal requirements to consider information security within the project lifecycle
c) There is insufficient information security expert involvement in projects
d) Education on security principles and practices relevant to project related activities is inadequate
e) Project security risk evaluations do not occur consistently.

5.2.2.2 Recommendations

a) Establish more explicit information security review points in the project lifecycle
b) Provide more guidance on information security in the existing project methodology and project documents and templates
c) Enhance project management and delivery.

5.3 Commentary on the Phase 2 Report

Again, we see strong alignment between the findings and recommendations of the MSD report and the findings herein. Themes relating to the need for executive level consideration of information security, the need to establish role accountabilities, the need to implement enterprise risk management, the lack of visible controls and the need for standards alignment are all consistent. There are also similarities with our review of the in-scope systems and the Phase 2 review findings relating to how agencies undertake projects – for example the need for privacy and security assessments within the lifecycle of a system.

6 Advice to agencies

The advice we provide in this section is a non-exhaustive set of actions and considerations for Chief Executives to lift agency capability in respect to security and privacy. It should be noted that this is general advice – as we found in Section 4, there are examples of good practice being undertaken within the state sector.

6.1 Treat security as a business issue rather than an IT issue

In Section 4 we found responsibility for security is largely seen to lie with IT staff, and that security risk management is not integrated with the wider enterprise risk management processes operated by agencies. This would indicate that security is being seen predominately as an IT issue, rather than a wider business issue.

Security should be treated as a business issue, with appropriate executive sponsorship and oversight, rather than solely an IT issue. Information is a business asset and should be protected in accordance with its value to the organisation and, in the case of personal data, the individual. As a consequence, it would be expected that security should be a governance level issue, similar to other key business issues.

While the IT function has a key role in managing security, it should not be perceived as solely an IT issue. The responsibility for security of IT systems should lie with the business owners of the systems, rather than with IT (who are the custodians of the systems).

Other business functions within an agency play a key role in maintaining effective security. This includes, for example, human resources, facilities management and internal audit.

6.2 Link security practices to privacy practices

As we found in Section 4, in most cases it does not appear that the potential privacy impact of systems is being formally considered. This may indicate that there are uncontrolled risks to personal data.

We recommend that clear, formal links should exist between an agency's security practices and its privacy practices. Effective privacy cannot be maintained without effective security. Without clear formal linkages, the likelihood is increased that the security practices and the privacy practices are not sufficient to maintain the privacy of the individuals for whom the agency holds data.

As part of the linkage, Privacy Impact Assessments should be performed during development for any system that deals with personal information, and thereafter reviewed on a regular basis. This will help ensure that there is sufficient protection over the privacy of individuals' data within the systems, or accessible by the systems. The Privacy Commissioner has published a Privacy Impact Assessment Handbook[15] to guide organisations undertaking Privacy Impact Assessments.

6.3 Establish formal security governance structures and processes

As mentioned above we have found that many agencies lack comprehensive security policies, standards and procedures. This potentially indicates a lack of executive oversight, ability to consistently implement policy and integration with the wider organisational environment.

Formal security governance structures and processes should be established to provide a mechanism to govern security. The governance structures and processes should address the technology, people and process elements of security. The size and nature of the governance structures will vary from agency to agency.

[15] http://privacy.org.nz/privacy-impact-assessment-handbook/?highlight=privacy%20impact%20assessment

In developing security governance structures and processes, reference should be made to the following standards, which can be used as frameworks to help define and establish the governance structures and processes:

- The New Zealand Information Security Manual (NZISM), which is the baseline technical security policy and standards document for government departments and agencies
- COBIT (Control Objectives for Information and Related Technology), which is the widely recognised IT governance framework published by ISACA[16]
- The ISO/IEC 27000 series of standards relating to information security
- Security in the Government Sector (SIGS) policy[17] and the Protective Security Manual[18].

Security governance should also consider appropriate levels of oversight (second line of defence) mechanisms such as reporting structures (reporting on items such as security risk management metrics and security incidents), escalation processes and review points.

The security governance structures and processes should link into, and align with, the wider governance structures in place with the agency.

6.4 Ensure that roles and responsibilities for security are clearly defined and communicated

The findings in Section 4 showed mixed results in terms of defined and appropriate roles and responsibilities. In some cases this may indicate lack of executive accountability and oversight, confusion over roles and/or lack of separation of duties.

Roles and responsibilities for security should be formally defined, communicated and managed (via, for example, a performance management framework). The Chief Executive is responsible for security within an agency, but will delegate responsibilities and authorities to other agency staff. Important individual roles relating to information security include:

- **CISO** (Chief Information Security Officer) - The CISO should be a senior staff member (preferably within the Executive) who sets the strategic direction for security within the agency. Whether the CISO role is a dedicated role will be dependent upon the agency size, the nature of the information being protected, and the risks posed.
- **ITSM** (Information Technology Security Manager) - The ITSM is a person in a senior position that acts as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. Whether the ITSM role is a dedicated role will be dependent upon similar factors to those for the CISO.
- **Privacy Officer** - The Privacy Officer is familiar with the privacy principles in the Privacy Act; deals with privacy requests, complaints and breaches; trains other staff about privacy, and advises on privacy impacts and practices.

6.5 Ensure that formal security risk management practices in place

We found in Section 4 that many agencies did not have formal security management practices. This indicates that agencies may not be properly assessing and managing their security risks.

[16] ISACA is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. See http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[17] http://www.nzsis.govt.nz/publications/Security_in_the_Government_Sector_2002.pdf

[18] This is a classified document.

Formal security risk management practices should be in place to provide a structured process to manage the security related risks faced by the agency. Having a formal systematic approach to managing security risks allows for:

- Risks to be clearly identified
- Risks to be assessed in terms of their likelihood of occurring, and the impact on the confidentiality, integrity and availability of the agency's information
- Security efforts and spend to focus on issues that present the greatest risk to the agency
- A structured process to follow in order to make decisions about risk treatments and risk acceptance
- The effectiveness of risk mitigation and remediation efforts to be evaluated
- Risks and the risk management process to be monitored and regularly reviewed
- Information to be classified appropriately.

The security risk management practices should:

- Integrate and roll up into the agency's overall risk management practices
- Consider security at an agency wide basis, and within specific systems and processes
- Align with generally accepted risk management frameworks, such as "ISO/IEC 27005 Information technology – Security techniques - Information security risk management".

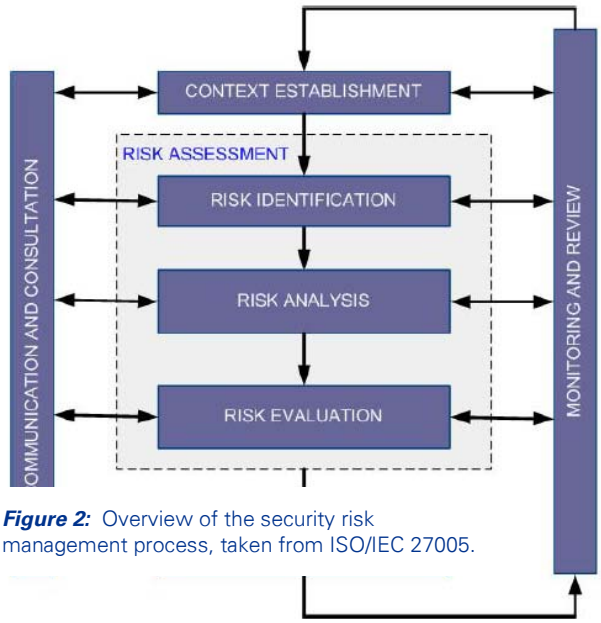


Figure 2: Overview of the security risk management process, taken from ISO/IEC 27005.

Figure 2 from ISO/IEC 27005 provides an overview of the key elements of a security risk management process.

These elements also align with those in the "ISO 31000 Risk management – Principles and guidelines" standard, which is commonly used by agencies to base their enterprise wide risk management processes upon.

6.6 Ensure that formal security policies, along with corresponding standards and procedures, are in place

As discussed above, many agencies lack comprehensive security policies, procedures and frameworks. We also found that many agencies did not have formal security risk management in place. These factors indicate that security risks are potentially not being properly considered and/or that security risk management are not integrated with the wider enterprise risk management framework.

A set of formal security policies, standards and procedures should be in implemented.

While most agencies have a security policy and a range of security procedures, few have security standards to link the policy to the procedures.

To provide a flexible solution, we suggest that a hierarchical structure for the policies, standards and procedures is developed, as depicted in Figure 3.

- **Security policies** specify management's intentions, grants authority, defines roles and responsibilities, provides definitions, and establishes high-level requirements while remaining technology neutral. Examples include a Security Policy and an Acceptable Use Policy. Security policies are relevant to all staff.
- **Security standards** provide technology-specific implementations of functional policies that help fulfil policies' objectives. Examples include a Password Standard, a Web Application Security Standard and a Database Security Standard. Security standards are relevant to systems administrators, security staff and systems developers.

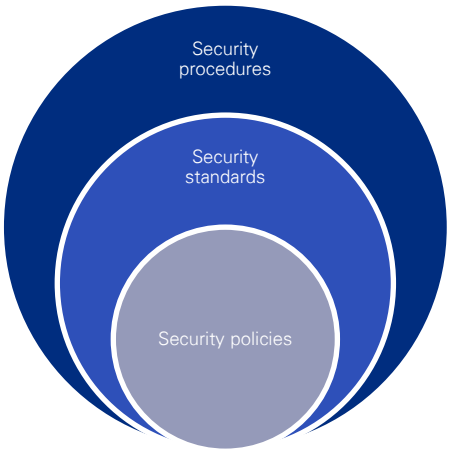


Figure 3: The hierarchical structure of security policy, standards and procedures.

- **Security procedures** provide step-by-step instructions for staff to implement defined security standards. Security procedures include system configuration instructions, and user provisioning instructions. Security procedures are relevant to systems administrators, security staff and helpdesk staff.

In addition to the policy framework, security practices provide cultural norms to support policies, standards and procedures. They include active support and modelling of security and privacy issues by the executive team, and mechanisms to foster a culture of risk, security and privacy awareness within the organisation.

This hierarchical framework provides the following benefits:

- **Security policies as a framework** - dividing the security management requirements from how they are actually implemented creates an extensible framework with the flexibility to specifically address current and future practices
- **Clear expectations simplify management** - with a concise and agreed source of security management requirements, it is easier for IT to link their security-related activities to business requirements
- **Maintenance should require less review** - the whole of the IT management group (and other members of senior management) are not required to be involved in every documentation update when standards-level technical details change
- **Clear expectations simplify compliance** - regulatory requirements and internal audit control measurements can be mapped to the consolidated security management requirements which can help to simplify compliance.

For smaller agencies, the policies, standard and procedures may be rolled up into one or two layers.

In terms of publicly accessible systems, agencies with Internet facing publicly accessible systems should give priority to developing a web application security standard to provide a basis to secure web based applications.

Where third parties are involved in the management or development of the IT systems, the security standards can be used as a mechanism to help articulate the agency's security expectations, and provide a basis against which to measure compliance.

6.7 Build privacy and security into the agency's Systems Development Lifecycle (SDLC)

We found in Section 4 that many systems lacked security design documentation. This indicates that such security design practices are not part of agency's standard Systems Development Lifecycle.

The Systems Development Lifecycle (SDLC) followed by an agency when developing new IT systems should have security considerations built into it.

At a broad level, security should be integrated into at least five different stages through-out the SDLC process. These are:

- **Requirements** – Risk assessment and security requirements analysis should be performed at the requirements stage to identify the key security elements that should be built into the system
- **Design** – A detailed security design should be developed during the design stage to identify the specific security controls to be implemented into the system
- **Testing and Evaluation** – Testing should be performed to test that the robust security is implemented prior to deployment
- **Operate** – Risks should continue to be reviewed and assessed post-deployment and controls reviewed and tested for their ongoing appropriateness and effectiveness as systems and external environment changes
- **Decommission** – Obsolete and unused systems should be actively decommissioned (and, where relevant, sanitised) to reduce the risk of security exposures.

In developing the security design, both application and infrastructure level risks and controls should be considered. The security designs observed usually address infrastructure level risks and controls, but give limited consideration to application level risks and controls.

For web based applications, in evaluating the application level risks and controls, consideration should be given to the guidance developed by OWASP (Open Web Application Security Project[19]).

6.8 Build security into the agency's system procurement processes

The findings in Section 4 relating to use of third party systems indicate that agencies may not be formally assessing the security of these systems.

It is important that security is formally considered when purchasing "off-the-shelf" systems. Security should be integrated into at least two different stages during the procurement process. These are:

- **Requirements** – Risk assessment and security requirements analysis should be performed at the requirements stage to identify the key security elements that should within the system. A requirement could include, for example, security certification.
- **Testing and Evaluation** – Testing should be performed to test that robust security is implemented prior to use. This should include an assessment of support processes and systems.

Particular focus should be given to "cloud" based systems. "Cloud", or cloud computing, refers to a business model whereby third party IT systems are provided as a service over the Internet. Agencies commonly use cloud based systems for recruitment, for example.

The security of agency information stored within a third party system is the responsibility of the agency and it is important to assess the provider's security arrangements against agency requirements.

[19] www.owasp.org

6.9 Establish a framework and process to certify and accredit systems

A formal framework and process to certify and accredit systems should be established. Such a framework is incorporated into the NZISM.

System certification refers to the formal assertion that an IT system complies with minimum security standards. System accreditation refers to the formal approval for a system to operate in production, with certification being a prerequisite for accreditation.

The certification and accreditation process should be followed whether a system is developed, or purchased off-the-shelf.

6.10 Ensure appropriate assurance is being sought

As part of an agency's security risk management practices, assurance should be gained over the design and operating effectiveness of the security controls in place.

The type and level of this assurance should depend upon the nature of the system being implemented, and should be defined within the agency's security risk management framework. For systems that present a higher inherent risk, for example, it would generally be expected that assurance is gained from independent security specialists.

In addition agencies should establish a security assurance framework to ensure they are gaining sufficient coverage and depth of assurance across their systems, and the internal audit function should be considering information security and privacy as part of its internal audit plan.

6.11 Consider an information management context to security

Consideration should be given to applying an information centric approach to security so that information assets can be governed, managed and leveraged according to their attributes.

The shift from managing attributes (security, privacy, archival requirements etc) to managing information asset classes has the potential to both decrease compliance costs as well as increasing the sector's ability to better leverage its information assets.

The benefits of having more accessible, better managed information assets include more evidenced based public policy, better performance management and better decision making.

The Data Management Association[20] has a number of useful resources to assist agencies with taking an information centric approach.

[20] www.dama.org

Appendix I – GCIO Terms of Reference

GCIO Review of Publicly Accessible Systems

Terms of Reference

The Government Chief Information Officer (GCIO), together with an external specialist, will review policy, process and assurance information provided by departments relating to the security of publicly accessible agency systems.

1) Remit

a. The Government Chief Information Officer ("GCIO") has been requested by the State Services Commissioner to review the security of publicly accessible systems across government

2) Purpose

a. provide Ministers with assurance on the security of publicly accessible systems

b. provide Chief Executives with advice on security improvements which can be made in the deployment and operation of such systems

3) Agencies in Scope

a. Public Service Departments, NZ Police and relevant Crown Entities

4) Matters in Scope

a. Publicly accessible systems including:

   i. Kiosks or similar devices that provide public access that are connected to a government network

   ii. Web servers that provide a service delivery interface

   iii. Wireless networks providing access to the public

5) Approach

a. Review:

   i. Lessons learned from MSD

   ii. Agency self-review reports

   iii. Agency documentation including:

      a) Information Management security policy and practices

      b) Change & Release Management processes

      c) Network and Security architectures

      d) Security and penetration tests and responses to those

      e) Audit reports and responses to those

b. Recommend:

   i. Identify systemic issues

   ii. Provide assurance

   iii. Provide advice on improvements

6) Timeframe

a. Draft report prepared by 27 November 2012

Appendix II – Agencies in Scope

Public Service Departments

- Ministry of Business, Innovation, and Employment
- Canterbury Earthquake Recovery Authority (CERA)
- Department of Conservation
- Department of Corrections
- Crown Law Office
- Ministry for Culture and Heritage
- Ministry of Defence
- Ministry of Education
- Education Review Office
- Ministry for the Environment
- Ministry of Foreign Affairs and Trade
- Government Communications Security Bureau
- Ministry of Health
- Inland Revenue Department
- Department of Internal Affairs
- Ministry of Justice
- Land Information New Zealand
- Ministry of Māori Development
- New Zealand Customs Service
- Ministry of Pacific Island Affairs
- Ministry for Primary Industries
- Department of the Prime Minister and Cabinet
- Serious Fraud Office
- Ministry of Social Development
- State Services Commission
- Statistics New Zealand
- Ministry of Transport
- The Treasury
- Ministry of Women's Affairs

Non-Public Service Departments in the State Service

- New Zealand Police

Non-Public Service Departments in the Wider State Sector

- Office of the Clerk of the House of Representatives
- Parliamentary Service

Crown Agents

- Accident Compensation Corporation
- Auckland District Health Board
- Bay of Plenty District Health Board
- Canterbury District Health Board
- Capital & Coast District Health Board
- Careers New Zealand
- Civil Aviation Authority of New Zealand
- Counties-Manukau District Health Board
- Earthquake Commission
- Environmental Protection Authority
- Hawke's Bay District Health Board
- Housing New Zealand Corporation
- Hutt Valley District Health Board
- Lakes District Health Board
- Maritime New Zealand
- MidCentral District Health Board
- Nelson-Marlborough District Health Board
- New Zealand Antarctic Institute
- New Zealand Blood Service
- New Zealand Fire Service Commission
- New Zealand Qualifications Authority
- New Zealand Trade and Enterprise
- New Zealand Transport Agency
- Northland District Health Board
- South Canterbury District Health Board
- Southern District Health Board
- Tairawhiti District Health Board
- Taranaki District Health Board
- Tertiary Education Commission
- Waikato District Health Board
- Wairarapa District Health Board
- Waitemata District Health Board
- West Coast District Health Board
- Whanganui District Health Board

Autonomous Crown Entities

- Commission for Financial Literacy and Retirement Income
- New Zealand Lotteries Commission
- Public Trust

Independent Crown Entities

- Electoral Commission

Appendix III – Summary of High Priority Unresolved Vulnerabilities

The following is a summary of the unresolved high priority issues identified for the systems in scope. These issues (beyond the connection of kiosks directly to internal networks) were identified by formal assessments commissioned by the agencies. The rating of high priority for the issues is based upon the rating applied within the assessments undertaken by the agencies.

We identified 13 agencies with systems with potentially high priority unresolved vulnerabilities, which are summarised below.

System type	Issue description	Number of agencies
Kiosk	Kiosks directly connected to the internal network of an agency.	4
Internet based system	Weak controls in place relating to password quality, password reset or account lockout.	4
Internet based system	The ability exists to perform a Cross Site Request Forgery (CSRF) attack. CSRF is an attack method that allows unauthorised commands to be performed under the context of a user, by manipulating a user to click on a malicious web link, view a malicious email or similar.	1
Internet based system	The ability exists to perform a Cross Site Scripting (XSS) attack. XSS is an attack method that that allows unauthorised code to be run within a user's web browser, resulting in such outcomes as users' behaviour being manipulated, or sensitive authentication details being disclosed to third parties.	3
Wireless network	Multiple weaknesses identified in the wireless network used, including weaknesses within the encryption implemented	1

Appendix IV – GCIO Advisory Group Terms of Reference

Terms of Reference

Advisory Group for the GCIO Review of Publicly Accessible Systems

Role of Group

The role of the Advisory Group is to support the Government Chief Information Officer's Review of Publicly Accessible Systems. The purpose of the review is to provide assurance to Ministers on the security of publicly accessible systems that contain personal information and advice to Chief Executives on security improvements which can be made in the deployment and operation of such systems.

The key tasks of the Advisory Group are to:

- provide advice and input on the assessment of the findings of the review
- provide input on the recommendations for actions and next steps – both for GCIO and for agencies (including any implications for the Cyber Security Plan)
- provide input and advice on approaches to implement the recommendations of the Review

Membership

- Colin MacDonald (Chair), Government Chief Information Officer, Department of Internal Affairs
- Grant Fletcher, Deputy Director, Information Assurance and Cyber Security, Government Communications Security Bureau (GCSB)
- Helen Wyn, Director, Policy Advisory Group, Department of Prime Minister and Cabinet (DPMC)
- Erik Koed, Assistant Commissioner, State Services Commission
- Mike Flahive, Office of the Privacy Commissioner (Observer status)

Secretariat

The Secretariat for the group will be Anne Shaw, Senior Stakeholder Manager, OGCIO. Stuart Wakefield, Director of the OGCIO will also be in attendance at meetings. KPMG who is supporting the review will attend as required.

Key Dates

To align with the milestones of the review, it is anticipated that the group would need to meet three or four times during November. A detailed timetable for the Review will be circulated and discussed with the Advisory Group.

Contact us

Souella Cumming
Partner – Advisory
T +64 4 816 4519
E smcumming@kpmg.co.nz

Brent Chalmers
Director – Advisory
T +64 4 816 4818
E brentchalmers@kpmg.co.nz

Philip Whitmore
Director – Advisory
T +64 4 367 5931
E pwhitmore@kpmg.co.nz

www.kpmg.com/nz

KPMG