STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

Government Use of Offshore Information and Communication Technologies (ICT) Service Providers

Advice on Risk Management

April 2009

New Zealand Government

State Services Commission
PO Box 329, Wellington, New Zealand

April 2009
ISBN 978-0-478-30366-7 (PDF)
ISBN 978-0-478-30365-0 (HTML)
Crown Copyright ©

 This work is licensed under a Creative Commons Attribution 3.0 New Zealand License. A summary of the key terms of that License, as well as its full legal terms, can be found online at: http://creativecommons.org/licenses/by/3.0/nz/

Contents

Note: all publications referred to in this document are hyperlinked in the text and are listed with their full URL in the Resources section. Academic footnotes are not used.

An earlier version of this document was published as*: Government Use of Offshore Information and Communications Technology (ICT) Service Providers: Interim Guidance.* October 2008.
ISBN 978-0-478-30354-4 (PDF), ISBN 978-0-478-30351-3 (HTML)

Introduction

Purpose

The New Zealand government is a steward of information and data on behalf of all New Zealanders. Stewardship requires an informed balance between sometimes competing drivers. Advances in technologies such as software-as-a-service, cloud computing, cost advantages of offshore service centres, or access to expertise and its transfer can make the use of offshore information and communication technologies (ICT) providers very attractive.

Conversely, agencies may dismiss potential opportunities to take advantage of these offerings because of uncertainty about their ability to meet obligations under legislation, regulation or policy.

This *Advice* is intended to provide agencies with basic information about possible risks related to transferring government information offshore or processing government information from a foreign location and to provide approaches to mitigating and managing those risks. It does not seek to prohibit the use of offshore ICT service providers. Whether the use of an offshore provider is desirable is ultimately a fact-specific decision for individual agencies. This *Advice* aims to assist agencies in making their own decisions.

Some of the advice is not unique to offshore outsourcing but also applies to outsourcing within New Zealand, particularly if the contractor is foreign owned or a target for foreign ownership.

Scope

The *Advice* is intended to be used as a resource when conducting risk assessments and developing risk management plans for proposed initiatives within existing policy frameworks for procurement, government security, and ICT project management. It does not create any new requirements but assumes and recommends the use of risk management approaches within existing frameworks.

It addresses principal risks to New Zealand's autonomy, authority and control over government information systems and information assets that may accompany the use of offshore ICT service providers. It explains possible mitigations for those risks and proposes a risk management approach to addressing them. Risks covered include, among other things, the security and integrity of personal and government information, continuity of service, trust and public confidence.

The *Advice* does not apply to contracting for software development or similar activities if they do not involve either transferring government information offshore or processing government information from a foreign location. Likewise, formal secure networks where risks are already fully or sufficiently mitigated are excluded from the scope.

Existing policy frameworks

Procurement and ICT project management frameworks

Departments have obligations under the *Mandatory Rules for Procurement by Departments* to conduct open and transparent procurement that respects New Zealand's non-discriminatory agreements with other countries. Clause 1 of those rules stipulates:

> These Rules set out mandatory standards and procedural requirements for the conduct of procurement by government departments (defined for this purpose as the "public service departments" listed in the Schedule to the State Sector Act 1988, plus New Zealand Defence Force and New Zealand Police). The Rules reflect and reinforce New Zealand's established policy of openness and transparency in government procurement. They are based on, but not limited to, the treaty obligations of New Zealand under Chapter 11 of the Trans-Pacific Strategic Economic Partnership Agreement with Brunei, Chile and Singapore (TPSEPA, also known as the P4 Free Trade Agreement). The Rules are to be applied by departments in their procurement globally to facilitate competitive participation by domestic and foreign suppliers in New Zealand's government procurement market.

Departments are also expected to abide by the *Policy Guide for Purchasers* produced by the Ministry of Economic Development and best practice guidance from the Auditor General, such as *Procurement Guidance for Public Entities*.

Relevant ICT project management guidelines include the *SSC Guidelines for Managing and Monitoring Major IT Projects*, the *Government Web Site Outsourcing Guidelines* and the *Government Web Standards and Recommendations.* Large projects may also come under the Gateway Review Process.

Security requirements

All government departments and agencies must comply with New Zealand legislation, regulation, government policy and national standards. Where overseas offices are maintained, legislation and regulation in the host country must also be taken into account. Where foreign legislation and regulation appears to be in conflict with New Zealand legislation, regulation, policy or national standards, advice should be sought from New Zealand's information security authority - the Government Communications Security Bureau (GCSB).

Government departments and agencies must also note the requirements for the handling of official information and any information classified under New Zealand's protective marking scheme. These requirements are specified in the document Security in the Government Sector (SIGS). Where necessary, advice on these matters should be sought from the GCSB.

Security in the Government Sector (SIGS) states:

1. The Government requires that information important to its functions, its official resources and its classified equipment is adequately safeguarded to protect the public and national interests and to preserve personal privacy. …
2. Chief Executives and heads of government departments and agencies, State Owned Enterprises and Crown Entities are responsible for implementing and managing effective security arrangements within their organisations. They must create and maintain appropriate security environments to adequately protect official information and classified equipment. The level of protection must correspond to the assessed level

> of risk. (Security in the Government Sector. Department of the Prime Minister and Cabinet, 2002. Policy Statement, p. 5)

Government departments and agencies should note that SIGS is ***mandatory*** for all departments and is ***recommended*** for Crown entities. However, the requirement for Crown entities to comply with New Zealand legislation, regulation, government policy and national standards remains unchanged.

While standards and guidance on risk and ICT security from non-New Zealand sources may be helpful, these must be considered to be a supplement but ***may not*** supersede any New Zealand legislation, regulation, policy or standards.

Background

Government agencies considering the use of ICT service providers for data processing and management services or government data storage should assess the risks of doing so and compare those risks against any potential benefits. Some risks may be trivial, such as when an agency chooses to make older publications available electronically. Others may be such as to preclude any consideration of permitting the information to be stored offshore, such as national security information or sensitive personal information such as criminal records.

Agencies might consider using an offshore ICT provider for several reasons, such as a lack of capability in New Zealand, value for money, or anticipated technology and skills transfer to the agency from the offshore provider. While these potential benefits might exist, agencies should balance them against the risks that such offshoring might pose as below.

- **Loss of control.** Offshoring data or data processing and management services can limit the control that government agencies have over the quality and type of services provided. Foreign service providers, industry, infrastructure services and governments can exert influence over the way services are delivered, developed and protected. Government agencies are likely to have less control over data held offshore than over data held in New Zealand.
- **Loss of privacy and security.** The confidentiality of offshore ICT services can be threatened by factors outside the control or knowledge of the New Zealand government. Offshoring may make it difficult or impossible for NZ government agencies to monitor and manage security and privacy effectively. In some circumstances, foreign law may enable another government to gain access to private New Zealand information and services without the knowledge or authorisation of the New Zealand government. Some foreign legislation may preclude notification to clients if the foreign government agencies access those clients' data.
- **Jurisdictional issues.** Outsourcing data or data processing and management to offshore ICT service providers may impede the investigation or prosecution of privacy or security breaches because the New Zealand law that supports such investigations does not apply or may be specifically excluded by contract. Agencies should investigate the rules surrounding legal discovery in the relevant jurisdiction and understand the implications for their agency.

A comprehensive risk assessment will entail a different effort for different situations but will always require identification of the significant risks, controls and mitigating measures, and a decision about the management of each of those risks. The effort should be proportionate to those identified risks as well as the expected rewards.

The assessment involves considering:

- the nature of the information to be outsourced
- the nature of the processes to be outsourced
- the location of the service provider (relevant jurisdiction), and, if different,
- the location from which service will be supplied.

The main concerns for security, service integrity, stewardship, and privacy when data is outsourced overseas are these.

- Possible non-compliance by the government agency with New Zealand legislation and policies, including the *Privacy Act 1993* and the *Public Records Act 2005* and the possible non-application of such legislation (e.g. the *Privacy Act*) which would apply if the service provider were not offshore. Offshore hosts can potentially collect, store, aggregate, and sell or otherwise exploit government information including government held personal information without the same legislative restrictions and sanctions that would apply in New Zealand.
- Intelligence-gathering by foreign governments and foreign non-governmental entities that may affect the security of government information and the privacy of New Zealanders.
- Overseas judicial decisions that might require disclosure of New Zealand personal information held offshore, or allow the commercial use of that information.
- Overseas or international (e.g. undersea cables or satellites) infrastructure breakdowns, natural hazards, civil unrest, industrial unrest, criminal activity, or terrorism with a potentially greater impact than would occur if similar incidents occurred in New Zealand.
- Possible monitoring or enforcement difficulties when rights must be asserted overseas and/or against offshore entities.
- Recovery and/or secure disposal of government information, including private data and intellectual property relating to sensitive government processes, at the termination of an outsourcing relationship.

Risk management approach

Agencies are required to take a risk management approach when considering any outsourcing, including sending government ICT services or data outside New Zealand. The New Zealand Government's standard for risk management is *AS/NZS 4360* supplemented by *HB231 (Handbook 231)* which is a guide to applying this standard. Both of these documents may be purchased through Standards New Zealand. *ISO/IEC27005* is expected to supplement these documents at some point.

The identification of critical success factors and unacceptable risks should be undertaken prior to a detailed risk analysis to establish the minimum protections required and any specific circumstances in which the offshoring initiative should be abandoned.

The recommended risk assessment process is to:

- identify relevant risks, vulnerabilities and controls, and their likelihood and impact
- identify the relevant stakeholder communities, their concerns, and possible reactions to adverse events
- assess the identified risks, their likelihood and impact
- identify existing or planned mitigations for each risk, and
- assess the residual (untreated) risk based on the reduced impact and/or likelihood that results from mitigation (Risk – Controls = Residual Risk).

A risk report about sending government ICT services or data offshore should include:

- the proposed location and its specifics such as: whether it is a European Union (EU) member state (and if it implements the EU Privacy Directive), languages normally used, and how it is rated by Transparency International, an international organization concerned with open and transparent government
- contract specific information such as (where applicable) the service that is being hosted or provided, what information is to be transferred between NZ and the provider, what primarily NZ-held information is to be processed remotely by the offshore service provider and the classification level(s) of any information involved
- the means of information transmission – how, when , what protections are applied
- the means of data recovery on termination of contract
- the management of test data for the service – what will be used, how it will be handled, how it will be safely disposed of when the test is over.

Ideally such a risk assessment should be undertaken before any procurement activity starts. Agencies should then assess whether the level of residual risk is acceptable. Under some circumstances, the risk will be considered unacceptable irrespective of any assessed monetary benefit. (See: Big picture risks)

A cost/benefit analysis can then determine the net benefit of offshoring ICT services, taking into account:

- the cost of the offshore contract and the cost of mitigating associated risks
- the residual (untreated/accepted) risks
- the expected benefits that will be realised through an offshore contract.

Ongoing risk management of an offshore contract

The final stage in the process is to define and implement management processes and governance structures to ensure that risk is managed throughout the life of the contract and possibly beyond. Change – political, legislative, business, systems, environmental, and cultural – is happening at an increasingly rapid rate and constant vigilance is needed to ensure that the ongoing risk, new risks that appear, and the impact of change is appropriately managed.

Agencies are reminded that regular, if not annual, reviews of risks and their mitigations/controls are good practice in any outsourcing arrangement. Those reviews should include whether any functions that have been outsourced might be (or have been) considered for secondary outsourcing, that is, sub-contracting, by the contractor. It is advisable for outsourcing contracts to prohibit the contractor from sub-contracting any of the outsourced tasks without the explicit written consent of the government agency.

Additionally, government agencies should not find themselves in the position where penalties arising from insufficiently flexible contract terms act as significant constraints on their ability to act in New Zealand's best interests.

Training and resources

Government Technology Services (GTS) provides risk assessment, risk management and security expertise. http://gts.ssc.govt.nz/risk-management/

GTS also provides training for government staff in applying the all-of-government *Risk Assessment* framework based on the *AS/NZS4360 Risk Management* standard. The workshop is aimed at those responsible for risk management either as part of a project or on a routine basis. While the training is generic, participants are encouraged to bring concrete examples for discussion. The email contact for this training is: gts@ssc.govt.nz /

The Treasury provides guidance on preparing a cost benefit analysis.

Government agencies are strongly advised to take advantage of the expert risk assessment panel established by SSC for Quantitative Risk Analysis (QRA) services for the preparation or review of a risk analysis where appropriate.

Agencies are also advised to consult their monitoring agencies as appropriate to endorse or advise on the risk assessment and cost/benefit analysis. For major IT projects, agencies should consult the *SSC Guidelines for Managing and Monitoring Major IT Projects* and the *Gateway Review Process*.

Agencies are reminded that the *Government Web Standards and Recommendations* apply regardless of whether their website is hosted in New Zealand or offshore.

Agencies should also note the requirements of the *Government Web Site Outsourcing Guidelines*. These are guidelines for NZ government agencies tendering and contracting for web development and hosting services.

Copies of Security in the Government Sector (SIGS) and the NZ Security in Information Technology guidance (NZSIT 40x) are available here. Government organisations requiring advice or training related to the application of these documents should contact liaison@gcsb.govt.nz in the first instance.

Discussion of key risks

The categorisation of risks below is a starting point for preparing the detailed risk analysis of an offshore contract.

They should not be considered as either a complete or accurate reflection of all of the risks and mitigations that might exist in the unique circumstances relating to an agency's decision about an offshore contract. Instead, agencies should build on and amend the identified risks through internal and external consultation to capture all relevant risks and mitigations.

The risks discussed on the following pages are:

Big picture risks: risks that may put a proposal out of consideration regardless of its other virtues.

Trust and public confidence risks: how a proposal may adversely affect the Trusted State Services Development Goal for the New Zealand State Services.

Control risks: the need to maintain control over data as required by, for example, the Public Records Act 2005.

Governance, management, and project risks: difficulties that may arise when management of a business function or project is geographically dispersed.

Economic risks: following procurement policy while considering possible effects on the larger New Zealand economy of an offshore proposal.

Business continuity risks: government responsibilities in maintaining capability in the country in the event of an emergency or a service provider failure.

Security and integrity risks: includes industrial espionage, social disruptions, terrorist threats, and data corruption.

Privacy risks: threats to government held personal information if sent offshore.

Legal, jurisdictional and commercial risks: practical and legislation-related risks of doing business outside New Zealand.

Fiscal risks: currency fluctuations, offshore taxes, and other financial risks.

Big picture risks

Some risks are sufficiently serious to warrant being described as "show stoppers". These would typically relate to the integrity and reliability of the legal system in the target jurisdiction. One guide to the relative risk of countries' integrity can be found in the annual *Global Corruption Report* at Transparency International's website. A second would be any formal advice from the Government Communications Security Bureau (GCSB) or the New Zealand Security Intelligence Service (NZSIS) on security hazards around hardware, software, or services from certain countries.

A different warning flag could be the existence of legislation which could allow foreign governments to silently take New Zealand Government data which was within their borders.

Government's role as a steward of information held on behalf of all New Zealanders requires that agencies take into consideration not just the impact on their agency but how their actions will impact other agencies that may require access to that information and the individuals and organisations that are the subjects of the information. Decisions that might be perfectly acceptable in isolation may become questionable when viewed from an all-of-government or an all-of-New Zealand perspective.

Some information should perhaps never be considered as the subject of contracting with an offshore provider. Agencies are best placed to identify their own sensitive resources but such things as information vital to national security, sensitive personal information such as criminal records, and company confidential information provided under obligation, including intellectual property and trade secrets, would probably fall into that category. Agencies should consider the likely public reaction to a data breach of that information if they have any doubts about its suitability for outsourcing or sending offshore.

One way to address these concerns may be to consider worst case scenarios to bring the broader picture to light. Those scenarios could also be used to explore how the sensitivity of the information may change over time and whether the information in aggregate (and as that volume grows over time) may require better protection and more security than individual records might require.

After completing a comprehensive risk analysis, government agencies should assess also whether the level of residual (untreated) risk for any offshoring initiative is acceptable. Generally, the agency can make this assessment based on the expected benefits of the initiative and the agency's appetite for risk. Agencies need to bear in mind that there are certain risks and issues that cannot be accepted. Agencies should note the mandatory requirements for securing official and classified information (see *Security in the Government Sector* - SIGS and *NZ ICT Security Manual* NZSIT402).

Similarly, one needs to be mindful that the standard contract terms of multinational companies often contain indemnities in favour of those companies (in essence, an indemnity is a contractual provision by which the indemnifying party agrees to keep the other party harmless against loss for specified acts or defaults). Such terms can raise issues under the *Public Finance Act 1989*, section 65ZC of which renders it unlawful for any person to give a guarantee or indemnity on behalf of the Crown (defined principally as Ministers and departments) unless expressly authorised by an Act. Authorisation may be granted by the Minister of Finance under section 65ZD or the granting of an indemnity may be expressly

authorised by the Public Finance (Departmental Guarantees and Indemnities) Regulations 2007.

When considering whether the giving of a particular form of indemnity is authorised under those Regulations, one needs to be careful to compare the scope of the indemnity in question against the statutory wording, because standard form indemnities often exceed the statutory permission. Where that is the case, Ministerial approval would be required before the indemnity is given. The alternative is to endeavour to "negotiate out" the indemnity from the company's standard terms or reduce its scope so as to render it compatible with any statutory permission that may be available. Crown entities should note that separate indemnity provisions apply to them. These provisions can be found in sections 160 and 163 of the Crown Entities Act 2004 and regulation 14 of the Crown Entities (Financial Powers) Regulations 2005.

These standard contract provisions or terms and conditions may also stipulate a non-New Zealand choice of law and jurisdiction for the resolution of contractual issues and disputes.
Government agencies should also be cognisant of the government's foreign relations position with certain jurisdictions before entering into commercial negotiations there. For example, it may be inappropriate for a government agency to enter into commercial negotiations or contracts in the jurisdiction of a foreign government if the NZ government has officially protested against or condemned the actions of that government. Advice should be sought from the Ministry of Foreign Affairs and Trade in these circumstances. Note also that New Zealand government agencies, citizens and companies must comply with regulations implementing NZ Security Council sanctions.

Government agencies are advised to seek the opinion of monitoring agencies on any issues or risks that might be deemed unacceptable by government.

Trust and public confidence risks

"Trusted State Services" is one of the *Development Goals for the New Zealand State Services.* This goal is: *"New Zealanders have confidence in the people, systems and processes of the State Services and the way services are delivered. They trust that agencies will deliver the services they need to go about their lives."*

To establish and maintain this level of trust and public confidence, agencies must continue to protect the quality and security of government information and services, whether or not these services are provided or supported from offshore. Trust is hard won; it is easy to erode and difficult to re-establish. Perceived or actual breaches of quality or security in services outsourced offshore will reflect poorly on the governance and competence of the government agency involved and potentially the wider state sector. It is essential that government agencies are prudent about developing and managing any initiatives which would result in services or data moving offshore.

Trust and confidence in government can usefully be seen as second order effects of good information management practices. Threats to trust and confidence in government can arise not only from any actual leak or loss of data, but also from people's perceptions about the level of risk to their personal data or other sensitive data arising from government decisions to locate data or data processing services offshore. Media reports of data breaches outside New Zealand can affect perceptions of the safety of information held within New Zealand as well as information transferred offshore. In these situations public perception may be a more significant concern than an objective view of risk might suggest.

Government agency ICT relationships with regions, countries or operators that are perceived to be high risk may undermine public confidence in that agency. Furthermore, such perceptions can aggravate issues when a breach of trust and confidence has occurred, even if appropriate due diligence and risk management has taken place. For these reasons, it may be advisable to avoid dealings in areas in which the public has low levels of trust. Refer to the annual *Global Corruption Report* at Transparency International's website as one means of identifying areas of low public trust.

Two types of risk are possible when offshore providers are located in jurisdictions where there is no comprehensive privacy legislation or where data breaches may be difficult to investigate or terms of contracts enforced. They are the (objective) risk of a breach of people's privacy and the (perception) risk of damaged confidence in government. Concerns relate to:

- the storage and transmission of personal data, e.g. through hosting websites and undertaking transactional activities such as surveys
- the potential collection of personal data by offshore providers of search tools, e.g. through retaining records of people's search requests
- the collection and use of personal data for analysis purposes, e.g. web analysis tools which track a user's behaviour on websites
- the use of information collected by New Zealand government by other parties for purposes for which it was not collected, such as any use of New Zealand government databases for marketing or consumer profiling, or the aggregation of New Zealand government databases with other data for unauthorised purposes.

These specific mechanisms provide ways for personal data to 'leak' beyond the public sphere. In some cases, the amount of personal information that can leak is relatively small but small pieces of information can in principle be consolidated to provide more detailed dossiers of information about individuals. Conversely, even supposedly "anonymous" information, if collected in sufficient quantities, can unintentionally identify individuals. AOL (an international internet service provider) learned that lesson the hard way in 2006, when it released what it thought was anonymous data on over 650,000 people's search activities, but later found that from such bits of information, a "mosaic" could be created that could eventually lead to identification of an individual.

Trust and public confidence risks	Example mitigations
• Adverse effect on public trust in e-government services and government in general. • Loss of autonomy, authority and control, higher risk of data breaches. • Public perception that service or data offshore is riskier or unacceptable. • Loss of control over government information because it would be subject to the laws of other countries. • Trade relationships affected by loss of international confidence in New Zealand systems.	• Seek appropriate advice (e.g. from MFAT, DPMC, security agencies). • Seek Ministerial agreement before commencing negotiations. • Seek appropriate legal advice. • Investigate the scope and powers of foreign legislation over New Zealand data and services and offshore support personnel or providers. • Ensure effective security management. • Avoid offshoring private or sensitive data or services (including remote support) where assurance over the confidentiality of data cannot be assured. • Limit the scope of the service provider for downstream outsourcing.

Control risks

Agencies are not released from their obligation to obey New Zealand law and policy because they have outsourced data or operations to contractors in New Zealand or beyond.

Digital information created as part of an agency's functions is part of the public record to which the *Public Records Act 2005* applies. Agencies are also responsible for their handling of personal information under the *Privacy Act 1993*.

It is important that government maintains control over its information and how it is accessed and used, whether hosted within or beyond its jurisdiction. Offshore hosting of government information poses a risk of loss of control over such information. Particular care should be taken when agreeing to standard terms and conditions, to ensure that they do not have the effect of the agency either losing control of its data (e.g., through an assignment of copyright) or granting an exclusive or otherwise inappropriately broad licence to the service provider.

Control risks	Example mitigations
• Loss of control over data. • Loss of control over supplier or sub-contractor performance. • Loss of control over service delivery because of unreliable foreign national/international infrastructure. • Inadequate management of information and records created as part of government functions. • Loss of information or records due to non-recovery or lack of authorised disposal following end of contract.	• Seek appropriate legal advice. • Investigate the scope and powers of foreign legislation over New Zealand data and services and offshore support personnel and providers. • Specify requirements for the creation and maintenance of information and records in contracts. • Specify contractual agreements on recovery or disposal of information at the close of a contract. • Avoid offshoring private or sensitive data or services (including remote support) where assurance over the confidentiality of data cannot be assured. • Limit scope for further outsourcing by the service provider. • Contract and test for redundancy and business continuity.

Governance, management, and project risks

When services are hosted offshore, the government agency's management staff may be geographically remote from at least some of people who actually deliver the service. Similarly, business owners and governance groups for projects may be distant from the developers. In some cases, service delivery or project tasks will be split over multiple locations, which can complicate the management and integration of operations or fragment the service delivery supply chain or coordination of the various project components. When the governance team is isolated from the project team it may have difficulty remaining connected with project risks and issues.

Agencies geographically separate from their project or service functions may not be able to visit those teams. They may be wholly reliant on the supplier's reporting which may leave them poorly informed about project progress or service delivery issues. This can reduce the ability of government agencies to monitor and manage the risks, issues, day-to-day service delivery and project progress. Additionally, it may be difficult to ensure business requirements are understood and are being delivered appropriately. Service desks are often located in low labour-cost countries which may bring security concerns.

Accordingly, it is appropriate for government agencies to complement stringent performance expectations with rigorous measurement and review processes. Regular and comprehensive quality assurance reviews may be advisable. Agencies need to remain abreast of current and emerging issues and be able to respond as necessary.

Governance, management and project risks	**Example mitigations**
(Many of these risks are common to on-shore outsourcing as well.) *Governance and management* • Arm's length management. • Delays in identifying problems, adding to fallout. • Poor knowledge of service quality, issues and risks. • Low compliance with audit & other government requirements. • Fragmented governance team leads to misunderstandings. • Reporting difficulties. • Audit difficulties. *Project* • Organisational push-back and lack or cooperation.	*Governance and management* • Contract should include compliance with New Zealand government ICT project controls and audit requirements (see Resources section under risk management) . • Contract should include compliance with best practice (e.g. project methodology, ITIL) governance frameworks. • Contract for effective recording and reporting of issues, risks and non-compliance with government requirements. • Establish auditing and compliance checks as a performance measure affecting revenue. • Establish a governance team including New Zealand-based representatives of the offshore service provider. *Project* • Ensure the offshore service provider and government agency adopt a recognised 'best practice' project management methodology (e.g. Prince2, PMBoK).

Governance, management and project risks	Example mitigations
• Poor knowledge of: - product quality - issues and risks - project progress. • Interruption in service because of start-up and transition risks. • High exit costs and difficulty moving the project to new service providers because of knowledge capture by the remote service provider.	• Contract should include compliance with New Zealand government ICT project. • controls and audit requirements (see Resources section under risk management) . • Ensure ongoing project risk management and risk reporting. • Undertake regular offshore training of key staff to maintain fluency in the solution. If possible, maintain an overseas presence. • Establish a local capability and backup for services, perhaps by insisting on a local provider of support services. • Ensure effective change management so that documentation and training material is kept current and accessible. • Consider the long term strategic value to New Zealand of the skills being outsourced (consult the Department of Labour) . • Don't move strategic intellectual property offshore.

Economic risks

Sending government data and data processing and management overseas could pose risks to New Zealand's economic wellbeing and these may need to be weighed in the cost benefit assessment of the anticipated financial benefits of an initiative.

These risks include the threat of industrial espionage aimed at undermining or gaining advantage over the trade of New Zealand and its partners including theft of intellectual property. This type of activity can be more commonplace, harder to identify and harder to combat in foreign jurisdictions. As discussed under *Big picture risks*, the Ministry of Foreign Affairs and Trade is a source for advice on existing New Zealand Security Council sanctions or other formal protests or condemnations of another government's actions.

Other risks to New Zealand's economic wellbeing relate to the reliability of information and services that support New Zealand's trade and reputation. Compromised or unreliable services can have a detrimental effect on trusted relationships with business, consumers and governments. It must be noted that a catastrophic loss of trust in the services or data of one New Zealand government agency will almost certainly affect the reputation and effectiveness of other agencies.

Where appropriate, government agencies may also want to consider the strategic effect on New Zealand's labour force. Moving a specialised function offshore, especially when it is the only instance of this function being performed in New Zealand, could have a long term impact on New Zealand's capability in certain technical fields. In such circumstances the wider public good should be considered, perhaps with advice from the Department of Labour.

Moving large-scale operations offshore may also affect unemployment rates, the balance of trade and Crown revenue. A government agency's offshoring initiative, while not large-scale enough to have this direct effect, may provide motivation for a significant commercial operation in New Zealand to contract or move offshore. Where this risk is identified, advice should be sought from Treasury.

As a reminder, Government procurement policy requires:

- best value for money over whole of life
- open and effective competition
- full and fair opportunity for domestic suppliers
- improving business capabilities, including e-commerce capability; and
- recognition of New Zealand's international trade obligations and interests.

Economic risks	Example mitigations
• Failure to meet international obligations or comply with internal agreements. • Reduced economic benefit to NZ (This is balanced by FTAs, membership in APEC, OECD etc.). • Domestic capability reduced as technical teams and knowledge move offshore. • Balance of trade deteriorates and Crown revenue is reduced as large-scale production moves offshore. • Unemployment rates increase as producers move offshore. • Trade advantages lost and trade relationships affected by security breaches.	• Conduct all significant procurements in compliance with, where applicable, the *Mandatory Rules for Procurement by Departments* and other procurement advice from MED and the Auditor General. • Domestic capability maintained by having New Zealanders closely working with the offshore provider. • Don't move strategic intellectual property offshore. • Seek advice from the Department of Labour, Ministry of Foreign Affairs & Trade, and Treasury. • Ensure effective security management.

Business continuity risks

It might be argued that sending some services offshore can offer benefits in terms of capability such as access to offshore expertise. However, this needs to be seen against the risk of failure in a foreign operation causing service delivery failures in New Zealand.

The Reserve Bank has considered the risks of offshoring banking services and has established policy aimed at ensuring the continuity of banking services in the event of a service failure in a foreign jurisdiction:

> A large bank that outsources its business activities must also be able to continue to function in the event that its service provider fails or becomes dysfunctional, or in the case where the provider is a parent bank, becomes subject to the administration of a foreign supervisor. For both of these purposes, it is essential that the bank in New Zealand has access to the customer records, people and systems it needs to continue operating.

To a great extent, that same philosophy should be adopted by government agencies when offshoring ICT services. A government agency must be able to access the records, systems and services it needs to continue operating in the event of a service provider failure, infrastructure failure, government intervention, etc., in that foreign jurisdiction. Government agencies may want to review the Reserve Bank policy and develop their own strategy for dealing with similar service or systemic failures.

Business continuity risks	Example mitigations
• Loss of domestic capability including loss of organisational knowledge and strategic capability. • Loss of intellectual property – explicitly and embedded in system design or business processes. • Effect of loss of skilled jobs to a particular part of the New Zealand economy. • Limitations on future options due to loss of capability to develop alternatives. • New Zealand Government's capability to deliver service is reduced because: - There is a service level reduction compared to New Zealand providers. - Service providers may not have the understanding required of the New Zealand market, operating environment and local needs and preferences to deliver the best possible services. - Staff morale and productivity issues may arise because of impending changes. - There are difficulties in communicating performance expectations.	• Undertake regular offshore training of key staff to maintain fluency in the solution. If possible, maintain an overseas presence. • Establish a local capability and backup for services, perhaps by insisting on a local provider of support services. • Implement change management strategy & ensure effectiveness with training material and documentation kept current and accessible. • Undertake best practice governance, contract and service delivery management. • Investigate and contract for appropriate levels of technology redundancy, resilience and business continuity capability. • Consider the long term strategic value to New Zealand of the skills being outsourced (consult the Department of Labour). • Don't move strategic intellectual property offshore. • Quality and level of service is specified and managed by a service level agreement. • Structures and processes established to monitor and manage communications and performance expectations.

Security and integrity risks

The same risks to personnel security, physical security and ICT security exist in foreign jurisdictions as in New Zealand. However, the likelihood of those risks occurring in some places can be significantly higher because of economic, social and legal differences. Furthermore, the ability of a New Zealand government agency to manage those risks or an actual security breach can be frustrated by distance, language, contractual provisions and the absence of legal authority.

Industrial espionage by governments, commercial organisations or political extremists can be commonplace in foreign jurisdictions. These activities can be aimed at gaining advantage over New Zealand trade or the trade of New Zealand's economic partners. Significant financial incentives may be offered in return for compromising New Zealand's services and data. Agencies should also consider the potential for interest in their data from organised crime. In those jurisdictions, New Zealand may have insufficient control, as well as criminal or civil remedies to prevent or penalise such a compromise.

Threats to service integrity and accessibility of information can arise because offshore service delivery may be compromised by events or activities outside the control of the New Zealand government. This is particularly sensitive when continuous service is required, and could arise from technical failure of the service provider or from some industrial, social, political or physical event in the offshore supplier's country. In those situations, government information including personal information might be compromised or no longer available.

Similar concerns could arise from the application of foreign legislation, which may confer less protection than New Zealand's information and privacy laws. An offshore company will be subject to laws and regulations other than those of New Zealand.
Specific threats to the continuity of services relate to the extension of the supply chain to offshore locations. Offshoring services can introduce support issues because of differing time zones and languages. For example:

- While an offshoring contract might stipulate 24x7 help desk support, continuity of services in New Zealand business hours might be degraded when key second and third level support staff have, say, 2 hour response times or are only available remotely. Those second and third level support staff might also need to refer to other outsourced or third party staff that are inaccessible during New Zealand business hours.
- The distances involved introduce additional risks to infrastructure. For example, a government agency offshoring an ICT service significantly increases its risk of telecommunications infrastructure failure because it relies on both domestic and foreign telecommunications infrastructures. This may be exacerbated by the presence of "single points of failure" for which network resilience and redundancy cannot be provided.

These concrete concerns may be accompanied by less tangible concerns around, for example, compliance with the *Standards of Integrity and Conduct for the State Services*, specifically the requirement that "We must treat information with care and use it only for proper purposes."

Security and other stewardship concerns arise for reasons similar to some of the privacy concerns, i.e. the risk of information being lost, stolen (copied), corrupted, or provided to or compulsorily obtained by a foreign government or non-government (and possibly criminal) organisation. Clearly, copied and corrupted data are hazards wherever the data is held. However, because the loss, theft, or corruption of offshore data may not be immediately

obvious to the New Zealand Government, the potential damage from using corrupt data, identity fraud, or other misuse may be exacerbated because of delays in recognising the problem. Delay in being able to deal with problems and implement solutions in foreign jurisdictions is also a potential risk.

Concerns can also arise from the possibility that communicating with an offshore provider can create a risk that software applications or data transmissions could be corrupted or infected with viruses or other malware. The distances involved, time zones and language differences may all mean that threats and events are never identified properly or communicated to the New Zealand government agency. Similarly, the use of offshore facilities may place government data outside the support scope of any potential malware mitigation measures provided by the Centre for Critical Infrastructure Protection (CCIP). Jurisdictional issues may mean that New Zealand government agencies are unable to adequately identify, investigate, mitigate, and prosecute security breaches when they are identified. These risks apply to maintenance, support, and control from offshore even if the data remains in New Zealand.

Existing security classifications of government-held data may need to be reassessed on their possible increased value as an aggregated collection, rather than as individual pieces of information, if the data is to be located or processed offshore. There may also be valuable intellectual property encapsulated in the systems and business processes underlying the ICT functions and data. Cabinet approved a set of *Guidelines for the Treatment of Intellectual Property Rights in ICT Contracts* that were released in January 2008. The aim of those Guidelines is to make newly developed intellectual property rights more readily available to the New Zealand commercial sector.

As a practical example, while usually thought of as relatively innocuous, if a website is closely linked to an agency network, or it collects sensitive information, tools such as website analytics provided through an offshore server may introduce security risks:

- Unauthorised access to private or government data by individuals or organisations not subject to New Zealand law.
- The service provider's computer code or equipment supporting government websites might introduce security vulnerabilities to the government agency web server or to the visitor's computer.
- Communications between the client, the web server and the service provider might be intercepted, modified, spoofed or otherwise compromised.

Security and Integrity risks	**Example mitigations**
Security General • There is a risk of industrial espionage (initiated by government, commercial organisations or political extremists) aimed at gaining advantage over New Zealand trade or the trade of New Zealand's economic partners. Financial incentives in return for compromises of New Zealand services and data in other jurisdictions may have no criminal or civil remedies.	• Contract for compliance with New Zealand government security requirements. • Undertake regular threat assessments. • Train offshore service providers. • Regularly audit offshore service providers. • Establish a formal security governance structure. • Ensure appropriate security monitoring.

Security and Integrity risks	Example mitigations
• Non-compliance with New Zealand government security policy • Higher risk because of greater volume of information offshore (the classification of individual documents may not reflect value of a collection of information). • Non-compliance with *Protective Security Manual (PSM)*, impact on physical security, difficulties with enforcing physical security. • Non-compliance with other relevant NZ standards – standards applied may not agree with NZ standards. *Confidentiality* • Theft of hardware. • Theft of data or loss of data. • Insertion of backdoors or other extraneous code if software is developed offshore. • Intelligence gathering – commercial and by government(s), including aggregating New Zealand's Government's information about its citizens with information gathered by other means. • External threats – war, revolution, civil unrest, terrorist attack. *Availability* • Technical barriers, processes or policy that restrict access to data and services. • Theft of hardware. • Theft of data or loss of data. • Natural hazards such as earthquakes or civil infrastructure breakdowns (power, transport, telecommunications), or undersea cables cut.	• Ensure security incident management processes are in place at the offshore service provider and the government agency. • Contract and test for redundancy and business continuity. • Ensure consideration is given to the potential value of the information, when matched with other sources. • Establish Government agency business continuity planning in case of offshore service failures. • Ensure local backup for data and services in case of extended offshore service failures (e.g. natural disaster, war).
Integrity • Corruption of data – stored or in transmission. • Poor quality control over data input or processing. • Lack of sustainability of digital information. Digital information needs to be actively managed over time to ensure ongoing accessibility and usability. • Interception of communications or loss in transit (electronic, courier, etc).	*Integrity* • Establish and monitor data quality measures. • Ensure data quality and sustainability are covered in the contract.

Privacy risks

How government is seen to treat personal information contributes significantly to government's reputation as fair, transparent and trustworthy. In New Zealand the protection of personal information is provided for by the Privacy Act 1993. The international context of that legislation is generally irrelevant to its domestic operation. However, that context becomes important when offshore ICT services are considered. It is not as simple as saying that any transfer or collection by offshore agencies is bad or inherently risky to the privacy of New Zealanders.

The Privacy Commissioner recommends privacy impact assessments as the best practice tool for examining and documenting privacy risks and mitigations and publishes a free downloadable *Privacy Impact Assessment Handbook*.

In fact, while privacy legislation dates back to at least the 1970s, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* on which most modern laws are based, has its origins in concerns that differences in the treatment of personal information could lead to non-tariff trade barriers and impede the free flow of international trade. It is why the Organisation for Economic Co-operation and Development (OECD) and Asia Pacific Economic Cooperation (APEC) work on privacy is part of larger projects to encourage freer trade and electronic commerce internationally. That economic driver adds weight to New Zealand's responsibilities towards personal information as a signatory to the Universal Declaration of Human Rights.

For example, while the Privacy Commissioner has expressed concern about personal information being sent offshore in an address to the 2007 GOVIS Conference, she has also signed a *Memorandum of Understanding* with the Australian Privacy Commissioner on cross-border cooperation over privacy complaint investigations. The Commissioner's office also participates in a range of activities at APEC, Asia-Pacific Privacy Authorities (APPA), and through the OECD, designed to encourage international cooperation on protection of personal information. The Data Protection Pathfinder, an APEC initiative, is working towards promoting a framework of principles on how cross-border rules should work across economies.

Those international efforts to collaborate on cross-border data privacy complicate our advice by providing a moving target. APPA started as a trans-Tasman initiative and now includes Hong Kong, Korea, and last year Canada. All the international bodies mentioned above have active programmes and other organisations may have useful resources, such as the International Chamber of Commerce model contracts, that can be applied to mitigate privacy risks.

See: Privacy risks and example mitigations next page

Privacy risks	Example mitigations
• Unauthorised release of personal information. • Inability to provide legitimate access by the data subject to personal information. • Inability to cooperate with Privacy Commissioner over complaints of interference with privacy. • Inability of the Privacy Commissioner to investigate or enforce against offshore offenders. • Inability to guarantee the protection of personal information in foreign jurisdictions which do not have privacy/data protection laws. • Foreign laws which conflict with the Privacy Act or offer less protection for the privacy of personal information. - Some offshore locations may be less problematic than others. Countries whose privacy legislation is considered "adequate" under the *European Union Directive 95/46/EC* may provide acceptable protection for personal information but agencies should check on the applicability of that protection to information from New Zealand and on enforceability from outside the potential hosting country. - Conversely, some jurisdictions may have legislation that permits their government access to any source of personal information held in that country. The Privacy Act gives immunity to breaches of the information privacy principles outside New Zealand that result from an agency's compliance with foreign laws (Section 10). • The Commissioner reported on the implications of that immunity provision in *Necessary and Desirable* (1998) Chapter 2.18, and in updates to that report in April 2000 and January 2003.	• Consult with your agency's Privacy Officer (all agencies are required to have a Privacy Officer under s.23 Privacy Act). • Conduct a Privacy Impact Assessment before putting out a tender. • Consider not sending personal information offshore and not allowing offshore service providers to collect personal information from New Zealanders. • Consider whether the information covered by an offshore contract can be restricted to public and static information. • Know the technological capabilities of proposed offshore locations and their ability to deal effectively with connection loss. • Develop contracts to cover all eventualities, specifying forum and choice of law and have it reviewed for enforceability under private international law. Contracts can explicitly reference the Privacy Commissioner's guidance on handling data breaches. • Consider standard contractual frameworks such as those from the International Chamber of Commerce. The EU publishes *Standard Clauses for the Transfer of Personal Data to Third Countries* and has recently issued an opinion that addresses a chain of possible sub-processing operations rather than a single sub-contract. • OECD covers cross border disputes in *Recommendation on Consumer Dispute Resolution and Redress*. It says it is not limited to the examples used in the document but might equally apply to other situations. In June 2007 the OECD adopted its *Recommendation on the Cross-border Enforcement of Laws Protecting Privacy*. • The Privacy Commissioner provides information about international activities and contact information for her international colleagues and their organisations. • One reasonably up-to-date and inexpensive guide to the state of privacy laws around the world is the annual survey Privacy and Human Rights published by the Electronic Privacy Information Centre, a US-based NGO. • The European Commission publishes its formal findings on the adequacy of data protection in "third countries" (i.e. non-EU states) online at *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*.

Privacy risks	Example mitigations
	• The EU also has proposed a framework for Binding Corporate Rules that multi-national companies can adopt to ensure their intra-firm transfers of personal information are acceptable under the EU Directive. See the consultation documents and see the *Resources* section for the Working Documents. • The EU has an arrangement with the US government about personal information transfers called Safe Harbor. This permits companies to self-certify to the US Federal Trade Commission that they abide by certain principles in the handling of personal information. • The EU has also published *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries.*

Legal and commercial risks

It is legally and practically more difficult for a New Zealand government agency or the New Zealand courts to enforce a contract with an offshore service provider, compared to a contract with a local provider. This is to some extent due to the potential difficulty in enforcement of the contract or some intervention by authorities in the offshore provider's home jurisdiction. Furthermore, it may require the government agency to obtain specialist legal advice in that foreign jurisdiction with consequent substantial costs and timeframes.

An aggravating factor may be the existence of foreign laws that override New Zealand's requirements for privacy, security and service continuity. Examples of these include laws that allow foreign governments unrestrained access to the information systems and data within their jurisdiction.

Agencies may also want to be careful to check the financial health of the company with which they are planning to do business so as to guard against the risk of loss of service or investment, and the difficulty in pursuing claims abroad, in the event of the company's bankruptcy, liquidation or other financial difficulty.

Legal and commercial risks	Example mitigations
• Non-compliance by the offshore provider with New Zealand's legislative requirements – *Official Information Act 1982*, *Public Finance Act 1989*, *Privacy Act 1993*, *Public Records Act 2005.* • Subject to laws in another jurisdiction – simple differences in legislation or interpretation of laws, stability of laws, quality of legal system (independent judiciary), differences in standard contracts, choice of law in contracts, venue for disputes, laws affecting data privacy (e.g. *US Patriot Act*). • Software licensing risks – unlicensed use of software, outsourcer software needs to be installed on local systems, unlawful distribution of software. • International law implications of commercial contracts. • Costs and difficulty of any foreign legal court action. • Bankruptcy, takeover, merger of or further outsourcing by contractor. • Effort required for maintenance of New Zealand third party support relationships. • Poor or variable outsourcer performance. • Contract lock-in.	• Design contract to cover all eventualities including, where relevant, any unacceptable Terms and Conditions or Acceptable Use Policy in the offshore provider's standard contracts (see the section on topics to discuss with your legal advisors). • Where practicable, contract for New Zealand governing law and jurisdiction. • Check for indemnities that may be inconsistent with *Public Finance Act* and negotiate them out of the contract or seek Ministerial approval. • Engage appropriate legal advice for contracts under foreign law. • Consider the value of New Zealand assets of the offshore service provider and whether the existence of those assets is likely to encourage compliance with the contract and relevant NZ legislation. • Choose country very carefully - perform a risk analysis of host country and, where possible, the impact of likely legislative changes. • Understanding the process, costs, remedies and likely timeframes for litigation prior to contracting. • Consider alternative dispute resolution mechanisms, being mindful of the forum for such resolution and the nature of any institutional or other mediation or arbitration rules that may be proposed.

Legal and commercial risks	Example mitigations
	• Impose performance and non-compliance penalties. • Ensure sufficient opportunity exists for early termination of the contract due to poor performance. • Evaluate what is the best mode of operation with local support providers (e.g. prime/sub-prime contracts) . • Limit scope for further outsourcing by the service provider. • Consider the need for a financial surety and/or performance guarantees. • Investigate insurance options to cover the risk of service provider failure - note that this does not prevent risks to service continuity; adequate disaster recovery, business continuity and early termination arrangements may need to be in place. • Ensure sufficient financial reserves exist in case of litigation.

Fiscal risks

Offshore outsourcing can present unique financial risks. Contracts that include future payments in a foreign currency can be subject to exchange rate fluctuations. Financial hedging or limiting contracts to New Zealand dollar terms can help mitigate this risk. Offshoring contracts might also incur unexpected liabilities in the foreign jurisdiction (e.g. taxes).

Unclear, ambiguous or overly flexible contractual terms may result in uncontrollable cost increases. These can occur because of assumptions made about business practice norms or simply because the parties sought a flexible and adaptable relationship. Clear contractual terms and variation processes may be the best way to avoid misunderstandings and unexpected costs.

Fiscal risks	Example mitigations
• Currency fluctuations – cost movements exaggerated and fixed price contracts. • Lock-in risks - price changes by suppliers, high set up costs, high compliance costs, fixed prices achieved by varying quality in response to changing demands and conditions, costs of repatriation or transfer to another supplier. • Unplanned liabilities and costs (e.g. taxes).	• Consider money market hedging, forward contracts and option hedging for significant future payments. • Implement contractual controls on price changes by suppliers. • Contract for flexibility to reflect changing financial market conditions. • Engage expert advice on the legal/financial concerns in the foreign jurisdiction.

Summary of key risks and mitigations

Risk	Example mitigations
Trust and public confidence risks • Adverse effect on public trust in e-government services and government in general. • Loss of autonomy, authority and control, higher risk of data breaches. • Public perception that service or data offshore is riskier or unacceptable. • Loss of control over government information because it would be subject to the laws of other countries. • Trade relationships affected by loss of international confidence in New Zealand systems.	• Seek appropriate advice (e.g. from MFAT, DPMC, security agencies) . • Seek Ministerial agreement before commencing negotiations. • Seek appropriate legal advice. • Investigate the scope and powers of foreign legislation over New Zealand data and services and offshore support personnel or providers. • Ensure effective security management. • Avoid offshoring private or sensitive data or services (including remote support) where assurance over the confidentiality of data cannot be assured. • Limit the scope of the service provider for downstream outsourcing.
Control risks • Loss of control over data. • Loss of control over supplier or sub-contractor performance. • Loss of control over service delivery because of unreliable foreign national/international infrastructure. • Inadequate management of information and records created as part of government functions. • Loss of information or records due to non-recovery or lack of authorised disposal following end of contract.	• Seek appropriate legal advice. • Investigate the scope and powers of foreign legislation over New Zealand data and services and offshore support personnel and providers. • Specify requirements for the creation and maintenance of information and records in contracts. • Specify contractual agreements on recovery or disposal of information at the close of a contract. • Avoid offshoring private or sensitive data or services (including remote support) where assurance over the confidentiality of data cannot be assured. • Limit scope for further outsourcing by the service provider. • Contract and test for redundancy and business continuity.

Risk	Example mitigations
Governance, management and project risks (Many of these risks are common to on-shore outsourcing as well.) *Governance and management* • Arm's length management. • Delays in identifying problems, adding to fallout. • Poor knowledge of service quality, issues and risks. • Low compliance with audit & other government requirements. • Fragmented governance team leads to misunderstandings. • Reporting difficulties. • Audit difficulties. *Project* • Organisational push-back and lack or cooperation. • Poor knowledge of: - product quality, - issues and risks, or - project progress. • Interruption in service because of start-up and transition risks. • High exit costs and difficulty moving the project to new service providers because of knowledge capture by the remote service provider.	*Governance and management* • Contract should include compliance with New Zealand government ICT project controls and audit requirements (see Resources section under risk management). • Contract should include compliance with best practice (e.g. project methodology, ITIL) governance frameworks. • Contract for effective recording and reporting of issues, risks and non-compliance with government requirements. • Establish auditing and compliance checks as a performance measure affecting revenue. • Establish a governance team including New Zealand-based representatives of the offshore service provider. *Project* • Ensure the offshore service provider and government agency adopt a recognised 'best practice' project management methodology (e.g. Prince2, PMBoK). • Contract should include compliance with New Zealand government ICT project controls and audit requirements (see Resources section under risk management). • Ensure ongoing project risk management and risk reporting. • Undertake regular offshore training of key staff to maintain fluency in the solution. If possible, maintain an overseas presence. • Establish a local capability and backup for services, perhaps by insisting on a local provider of support services. • Ensure effective change management so that documentation and training material is kept current and accessible. • Consider the long term strategic value to New Zealand of the skills being outsourced (consult the Department of Labour). • Don't move strategic intellectual property offshore.

Risk	Example mitigations
Economic risks • Failure to meet international obligations or comply with internal agreements. • Reduced economic benefit to NZ (This is balanced by FTAs, membership in APEC, OECD etc.). • Domestic capability reduced as technical teams and knowledge move offshore. • Balance of trade deteriorates and Crown revenue is reduced as large-scale production moves offshore. • Unemployment rates increase as producers move offshore. • Trade advantages lost and trade relationships affected by security breaches.	• Conduct all significant procurements in compliance with, where applicable, the *Mandatory Rules for Procurement by Departments* and other procurement advice from MED and the Auditor General. • Domestic capability maintained by having New Zealanders closely working with the offshore provider. • Don't move strategic intellectual property offshore. • Seek advice from the Department of Labour, Ministry of Foreign Affairs & trade, and Treasury. • Ensure effective security management.
Business continuity risks • Loss of domestic capability including loss of organisational knowledge and strategic capability. • Loss of intellectual property – explicitly and embedded in system design or business processes. • Effect of loss of skilled jobs to a particular part of the New Zealand economy. • Limitations on future options due to loss of capability to develop alternatives. • New Zealand Government's capability to deliver service is reduced because: - There is a service level reduction compared to New Zealand providers. - Service providers may not have the understanding required of the New Zealand market, operating environment and local needs and preferences to deliver the best possible services. - Staff morale and productivity issues may arise because of impending changes. - There are difficulties in communicating performance expectations.	• Undertake regular offshore training of key staff to maintain fluency in the solution. If possible, maintain an overseas presence. • Establish a local capability and backup for services, perhaps by insisting on a local provider of support services. • Ensure effective change management so that documentation and training material is kept current and accessible. • Undertake best practice governance, contract and service delivery management. • Investigate and contract for appropriate levels of technology redundancy, resilience and business continuity capability. • Consider the long term strategic value to New Zealand of the skills being outsourced (consult the Department of Labour). • Don't move strategic intellectual property offshore. • Quality and level of service is specified and managed by a service level agreement. • Change management strategy implemented. • Structures and processes established to monitor and manage communications and performance expectations.

Risk	Example mitigations
Security and integrity risks *Security General* • There is a risk of industrial espionage (initiated by government, commercial organisations or political extremists) aimed at gaining advantage over New Zealand trade or the trade of New Zealand's economic partners. Financial incentives in return for compromises of New Zealand services and data in other jurisdictions may have no criminal or civil remedies. • Non-compliance with New Zealand government security policy. • Higher risk because of greater volume of information offshore (the classification of individual documents may not reflect value of a collection of information). • Non-compliance with Protective Security Manual (PSM), impact on physical security, difficulties with enforcing physical security. • Non-compliance with other relevant NZ standards – standards applied may not agree with NZ standards. *Confidentiality* • Theft of hardware. • Theft of data or loss of data. • Insertion of backdoors or other extraneous code if software is developed offshore. • Intelligence gathering – commercial and by government(s), including aggregating New Zealand's Government's information about its citizens with information gathered by other means. • External threats – war, revolution, civil unrest, terrorist attack. *Availability* • Technical barriers, processes or policy that restrict access to data and services. • Theft of hardware. • Theft of data or loss of data. • Natural hazards such as earthquakes or civil infrastructure breakdowns (power, transport, telecommunications), undersea cables cut.	• Contract for compliance with New Zealand government security requirements. • Undertake regular threat assessments. • Train offshore service providers. • Regularly audit offshore service providers. • Establish a formal security governance structure. • Ensure appropriate security monitoring. • Ensure security incident management processes are in place at the offshore service provider and the government agency. • Contract and test for redundancy and business continuity. • Ensure consideration is given to the potential value of the information, when matched with other sources. • Establish Government agency business continuity planning in case of offshore service failures. • Ensure local backup for data and services in case of extended offshore service failures (e.g. natural disaster, war).

Risk	Example mitigations
Integrity • Corruption of data – stored or in transmission. • Poor quality control over data input or processing. • Lack of sustainability of digital information. Digital information needs to be actively managed over time to ensure ongoing accessibility and usability. • Interception of communications or loss in transit (electronic, courier, etc).	*Integrity* • Establish and monitor data quality measures. • Ensure data quality and sustainability are covered in the contract.
Privacy risks • Unauthorised release of personal information. • Inability to provide legitimate access by the data subject to personal information. • Inability to cooperate with Privacy Commissioner over complaints of interference with privacy. • Inability of the Privacy Commissioner to investigate or enforce against offshore offenders. • Inability to guarantee the protection of personal information in foreign jurisdictions which do not have privacy/data protection laws. • Foreign laws which conflict with the Privacy Act or offer less protection for the privacy of personal information. - Some offshore locations may be less problematic than others. Countries whose privacy legislation is considered "adequate" under the European Union Directive 95/46/EC may provide acceptable protection for personal information but agencies should check on the applicability of that protection to information from New Zealand and on enforceability from outside the potential hosting country. - Conversely, some jurisdictions may have legislation that permits their government access to any source of personal information held in that country. The Privacy Act gives immunity to breaches of the information privacy principles outside New Zealand that result from an agency's compliance with foreign laws (Section 10).	• Consult with your agency's Privacy Officer (all agencies are required to have a Privacy Officer under s.23 Privacy Act). • Conduct a Privacy Impact Assessment before putting out a tender. • Consider not sending personal information offshore and not allowing offshore service providers to collect personal information from New Zealanders. • Consider whether the information covered by an offshore contract can be restricted to public and static information. • Know the technological capabilities of proposed offshore locations and their ability to deal effectively with connection loss. • Develop contracts to cover all eventualities, specifying forum and choice of law and have it reviewed for enforceability under private international law. Contracts can explicitly reference the Privacy Commissioner's guidance on handling data breaches. • Consider standard contractual frameworks such as those from the International Chamber of Commerce. The EU publishes *Standard Clauses for the Transfer of Personal Data to Third Countries* and has recently issued an opinion that addresses a chain of possible sub-processing operations rather than a single sub-contract. • OECD covers cross border disputes in *Recommendation on Consumer Dispute Resolution and Redress*. It says it is not limited to the examples used in the document but might equally apply to other situations. • In June 2007, the OECD adopted its *Recommendation on the Cross-border Enforcement of Laws Protecting Privacy*.

Risk	Example mitigations
Privacy risks continued - The Commissioner reported on the implications of that immunity provision in *Necessary and Desirable* (1998) Chapter 2.18, and in updates to that report in April 2000 and January 2003.	• The Privacy Commissioner provides information about international activities and contact information for her international colleagues and their organisations. • One reasonably up-to-date and inexpensive guide to the state of privacy laws around the world is the annual survey *Privacy and Human Rights* published by the Electronic Privacy Information Centre, a US-based NGO. • The European Commission publishes its formal findings on the adequacy of data protection in "third countries" (i.e. non-EU states) online at *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*. • The EU also has proposed a framework for Binding Corporate Rules that multi-national companies can adopt to ensure their intra-firm transfers of personal information are acceptable under the EU Directive. See the consultation documents and see the Resources section for the Working Documents. • The EU has an arrangement with the US government about personal information transfers called Safe Harbor. This permits companies to self-certify to the US Federal Trade Commission that they abide by certain principles in the handling of personal information. • The EU has also published *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries.*
Legal, jurisdictional and commercial risks • Non-compliance by the offshore provider with New Zealand's legislative requirements – *Official Information Act 1982*, *Public Finance Act 1989, Privacy Act 1993*, *Public Records Act 2005.* • Subject to laws in another jurisdiction – simple differences in legislation or interpretation of laws, stability of laws, quality of legal system (independent judiciary), differences in standard contracts, choice of law in contracts, venue for disputes, laws affecting data privacy (e.g. *US Patriot Act*). • Software licensing risks – unlicensed use of software, outsourcer software needs to be installed on local systems, unlawful distribution of software.	• Design contract to cover all eventualities including, where relevant, any unacceptable Terms and Conditions or Acceptable Use Policy in the offshore provider's standard contracts (see the section on topics to discuss with your legal advisors). • Where practicable, contract for New Zealand governing law and jurisdiction. • Check for indemnities that may be inconsistent with Public Finance Act and negotiate them out of the contract or seek Ministerial approval. • Engage appropriate legal advice for contracts under foreign law. • Consider the value of New Zealand assets of the offshore service provider and whether the existence of those assets is likely to encourage compliance with the contract and relevant NZ legislation.

Risk	Example mitigations
Legal, jurisdictional and commercial risks continued • International law implications on commercial contracts. • Costs and difficulty of any foreign legal court action. • Bankruptcy, takeover, merger of or further outsourcing by contractor. • Effort required for maintenance of New Zealand third party support relationships. • Poor or variable outsourcer performance. • Contract lock-in.	• Choose country very carefully - perform a risk analysis of host country and, where possible, the impact of likely legislative changes. • Understanding the process, costs, remedies and likely timeframes for litigation prior to contracting. • Consider alternative dispute resolution mechanisms, being mindful of the forum for such resolution and the nature of any institutional or other mediation or arbitration rules that may be proposed. • Impose performance and non-compliance penalties. • Ensure sufficient opportunity exists for early termination of the contract due to poor performance. • Evaluate what is the best mode of operation with local support providers (e.g. prime/sub-prime contracts) . • Limit scope for further outsourcing by the service provider. • Consider the need for a financial surety and/or performance guarantees. • Investigate insurance options to cover the risk of service provider failure - note that this does not prevent risks to service continuity; adequate disaster recovery, business continuity and early termination arrangements may need to be in place. • Ensure sufficient financial reserves exist in case of litigation.
Fiscal risks • Currency fluctuations – cost movements exaggerated and fixed price contracts. • Lock-in risks - price changes by suppliers, high set up costs, high compliance costs, fixed prices achieved by varying quality in response to changing demands and conditions, costs of repatriation or transfer to another supplier. • Unplanned liabilities and costs (e.g. taxes).	• Consider money market hedging, forward contracts and option hedging for significant future payments. • Implement contractual controls on price changes by suppliers. • Contract for flexibility to reflect changing financial market conditions. • Engage expert advice on the legal/financial concerns in the foreign jurisdiction.

Some topics to discuss with your legal advisors

When contemplating contracting for services with an offshore supplier, agencies may wish to discuss the following issues with their legal advisors. The list below is not intended to be exhaustive and the importance and negotiability of such issues is likely to depend on the magnitude of risk and value of the contract.

- Procurement implications.
- Ensuring the contract deals appropriately with ownership and licensing of intellectual and other property, including personal information and other data and, where relevant, derivative works.
- The potential desirability of obliging the service provider to advise the New Zealand agency of any relevant changes in legislation, regulations and other controls on operations that are imposed on the provider by its home or operating jurisdiction.
- The potential need for clear definitions of terms, processes and behaviours that are significant to the operation of the contract and which, in the absence of clear definition, may be interpreted differently in the other jurisdiction.
- Prescribing contractual processes for handling project risks and issues and matters of change control.
- The potential need for provisions dealing clearly with matters of reporting, governance, audit, acceptance testing and liability.
- Considering the choice of law and forum for disputes, and the practical implications of these.
- The need for clear and appropriate escalation paths and dispute resolution processes.
- The potential need for change of ownership/control provisions.
- Where personal information is at stake, the desirability of data breach notification mechanisms.
- In significant projects, the potential need for a performance bond or guarantee.
- The potential application of, and compliance with, the *New Zealand Government Web Standards and Recommendations* and *Web Site Outsourcing Guidelines*.
- The potential desirability of including a prohibition on sub-contracting without the agency's express written consent.
- The advisability of carrying out a check on the financial health of the company with which they are planning to do business.

Resources

Training and resources in risk management

Government Technology Services (GTS) provides risk assessment, risk management and security expertise. http://gts.ssc.govt.nz/risk-management/

GTS also provides training for government staff in applying the all-of-government Risk Assessment framework based on the AS/NZS4360 Risk Management standard. The workshop is aimed at those responsible for risk management either as part of a project or on a routine basis. While the training is generic, participants are encouraged to bring concrete examples for discussion. The email contact for this training is: gts@ssc.govt.nz /

Risk Management AS-NZS 4360 2004
Information Security Risk Management Guidelines SNZ HB 231 2004
Both are available from Standards New Zealand at http://www.standards.co.nz/web-shop/?action=viewProductPack&mod=catalog&pid=4028828607e45bd10107fe3022980003&sectorId=I1
For government agencies, these are available through the Public Sector Intranet through an agreement between SSC and Standards New Zealand. https://psi.govt.nz/ims/default.aspx

The Treasury provides guidance on preparing a cost benefit analysis at http://www.treasury.govt.nz/publications/guidance/costbenefitanalysis/

Government agencies are strongly advised to take advantage of the expert risk assessment panel established by SSC for Quantitative Risk Analysis (QRA) services for the preparation or review of a risk analysis where appropriate (see http://www.e.govt.nz/resources/news/headlines/20080228.html/).

Agencies are also advised to consult their monitoring agencies as appropriate to endorse or advise on the risk assessment and cost/benefit analysis. For major IT projects, agencies should consult the *SSC Guidelines for Managing and Monitoring Major IT Projects* at http://www.ssc.govt.nz/ITguidelines and the *Gateway Review Process* at http://www.ssc.govt.nz/gateway.

Agencies are reminded that the *Government Web Standards and Recommendations* apply regardless of whether their website is hosted in New Zealand or offshore (see http://webstandards.govt.nz/).

Agencies should also note the requirements of the *Government Web Site Outsourcing Guidelines*. These are guidelines for NZ government agencies tendering and contracting for web development and hosting services (see http://webstandards.govt.nz/index.php/New_Zealand_Government_Web_Site_Outsourcing_Guidelines).

New Zealand legislation

The Parliamentary Counsel Office makes all New Zealand Acts and Regulations freely available at http://www.legislation.govt.nz/
Privacy Act 1993
Public Records Act 2005
Public Finance Act 1989 s.65ZC

International legal resources

WorldLii makes legislation from around the world freely available at http://www.worldlii.org/ Information is also made available by subject groupings such as privacy (including NZ privacy decisions, and case notes) http://www.worldlii.org/catalog/273.html and contracts http://www.worldlii.org/catalog/50048.html.

(European Union) *Standard Clauses for the Transfer of Personal Data to Third Countries* http://europa.eu/scadplus/leg/en/lvb/l14012.htm

(EU) Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

International Chamber of Commerce http://www.iccwbo.org/
Model clauses for use in contracts involving transborder data flows 23 September 1998 http://www.iccwbo.org/id911/index.html

New Zealand Government policies and standards

Standards of Integrity and Conduct for the State Services
http://www.ssc.govt.nz/display/document.asp?navid=311

Archives New Zealand
Continuum is Archives New Zealand's place to find resources and services, including advice, training and forums, on complying with the Public Records Act 2005.
http://continuum.archives.govt.nz/home.html

Ministry of Economic Development Procurement site
http://www.med.govt.nz/templates/StandardSummary____181.aspx
MED publishes *Mandatory Rules for Procurement by Departments* and *Policy Guide for Purchasers* on this site as well as other useful guidance. See in particular the basic principles in: http://www.med.govt.nz/templates/ContentTopicSummary____29393.aspx

Office of the Auditor General
Procurement Guidance for Public Entities http://www.oag.govt.nz/2008/procurement-guide/

Government Web Site Outsourcing Guidelines
http://webstandards.govt.nz/index.php/New_Zealand_Government_Web_Site_Outsourcing_Guidelines

Government Web Standards and Recommendations
http://webstandards.govt.nz/index.php/Home_page

Overseas Hosting Risk Analysis (for offshore web sites). http://www.e.govt.nz/policy/trust-security/overseas-hosting.html/view?searchterm=website hosting

Security in the Government Sector http://www.security.govt.nz/sigs/index.html

NZ ICT Security Manual NZSIT400 series http://www.gcsb.govt.nz/newsroom/nzsits.html

Guidelines for the Treatment of Intellectual Property Rights in ICT Contracts
http://www.e.govt.nz/policy/ipr

SSC Guidelines for Managing and Monitoring Major IT Projects
http://www.ssc.govt.nz/ITguidelines

The Reserve Bank's Policy on Outsourcing by Banks, by Tim Ng. Reserve Bank of New Zealand: Bulletin, Vol. 70, No. 2
http://www.rbnz.govt.nz/research/bulletin/2007_2011/2007jun70_2ng.pdf

Privacy resources

Privacy Impact Assessment Handbook, Office of the Privacy Commissioner
http://www.privacy.org.nz/privacy-impact-assessment-handbook/?highlight=PIA%20handbook

Privacy Breach Guidelines, Office of the Privacy Commissioner.
http://www.privacy.org.nz/privacy-breach-guidelines-2/

Privacy and Sovereignty: Data fight or flight. Speech by Marie Shroff, Privacy Commissioner at GOVIS, May 2007. http://www.privacy.org.nz/privacy-and-sovereignty-data-fight-or-flight-marie-shroff/

Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner.
http://www.privacy.org.nz/memorandum-of-understanding/

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

OECD Recommendation on Consumer Dispute Resolution and Redress
http://www.oecd.org/dataoecd/43/50/38960101.pdf

OECD Recommendation on the Cross-border Enforcement of Laws Protection Privacy (2007)
http://www.oecd.org/dataoecd/43/28/38770483.pdf

Asia Pacific Economic Cooperation Electronic Commerce Steering Group
http://www.apec.org/apec/apec_groups/committees/committee_on_trade/electronic_commerce.html This group is responsible for APEC work on privacy generally.
APEC Data Privacy Pathfinder
http://aimp.apec.org/Documents/2007/SOM/CSOM/07_csom_019.doc

Asia Pacific Privacy Authorities http://www.privacy.gov.au/international/appa/index.html

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

(EU) *Standard Clauses for the Transfer of Personal Data to Third Countries*
http://europa.eu/scadplus/leg/en/lvb/l14012.htm

(EU) Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

(EU) Binding Corporate Rules consultation documents
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/consultations/index_en.htm

(EU) Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp155_en.pdf

(EU) Working Document Setting up a framework for the structure of Binding Corporate Rules.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_en.pdf

(EU) Working Document Setting up a table with the elements and principles to be found in Binding Corporate Rules.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf

(EU) Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

International Chamber of Commerce http://www.iccwbo.org/
Model clauses for use in contracts involving transborder data flows 23 September 1998
http://www.iccwbo.org/id911/index.html

Privacy and Human Rights. An annual report from the Electronic Privacy Information Centre.
http://epic.org/bookstore/

WorldLii makes legislation from around the world freely available at http://www.worldlii.org/
Information is also made available by subject groupings such as privacy (including NZ privacy decisions, and case notes) http://www.worldlii.org/catalog/273.html

Reports

Development Goals for the State Services http://www.ssc.govt.nz/deveopment-goals

Transparency International's annual report on openness and transparency of governments around the world http://www.transparency.org

Canadian Privacy Commissioner *Report of Findings (2008 CIPPIC complaint)*
http://www.cippic.ca/uploads/OPC_Findings-canada.com.pdf .

Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing. Information & Privacy Commissioner for British Columbia ,October 2004. http://www.oipcbc.org/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf

AOL apologizes for release of user search data, by Dawn Kawamoto and Elinor Mills, CNET News, 7 August 2006. http://www.news.com/2100-1030_3-6102793.html

Dancing in the Minefield: Legal outsourcing abroad, by Sharon D. Nelson. http://ridethelightning.senseient.com/2008/09/dancing-in-the.html
See this article for discussion of an American Bar Association resolution on outsourcing legal services from outside the US.

A map of the world's undersea communications cables http://world-secure-channel.com/uploads/map_cables(1).jpg

Glossary of selected terms from HB 436:2004 and HB 167:2006

Risk
The chance of something happening that will have an impact on objectives.

Risk analysis
A systematic process to understand the nature of and deduce the level of risk.

Risk management framework
The set of elements of an organization's management system concerned with managing risk.

Risk management process
The systematic application of management policies, procedures, and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring, and reviewing risk.

Threat
Anything that has the potential to prevent or hinder the achievement of objectives or disrupt the processes that support them. A source of, or potential for harm to occur.

Vulnerability
Any weakness that can be exploited by an aggressor to make an asset susceptible to change