

Overseas hosting risk Analysis

RISK ANALYSIS

Issue: Hosting government websites overseas

The risk assessment will need to take account of:

- the reasons for going to offshore hosting, whether it is for lower costs, backup, quality of service, more advanced technology
- the location for offshore hosting
- what is being hosted, whether it is a relatively static site with public information, or is a dynamic service delivery site with personal or other classified information

Table of Risks and Mitigations

Risk Type	Risk Description	Mitigation/Comment
Legal	<p>Risk of not being able to comply with New Zealand's legislative requirements when hosting outside of New Zealand</p> <p>Examples include legislation relating to contracts, Privacy Act 1993, Official Information Act 1982, Public Finance Act 1989, Fair Trading Act 1986. For instance, many US contracts have very broad indemnity clauses, which may place you in breach of the Public Finance Act 1989 - Section 65ZC says: "except as expressly authorised by any Act, it is not lawful for any person to give a guarantee or indemnity on behalf of or in the name of the Crown".</p> <p>Risk of being subject to different laws in another jurisdiction</p> <p><i>Do not assume that local laws are equivalent to New Zealand especially when it comes to disputes and litigation. For instance, a court case in the US found that a hosting provider can make commercial use of customer information on their servers.</i></p>	<p>Design of contract to cover all eventualities, including the ISP or host Terms and Conditions and Acceptable Use Policy (which enable the site to be taken down if there are issues with the content)</p> <p>Deal only in public and static information</p> <p>Choose country very carefully - risk analysis of host country and the impact of likely legislative changes</p> <p>Management of software licences for COTS, customised and open source software</p> <p>Governance, contract and service delivery management</p>

Risk Type	Risk Description	Mitigation/Comment
	<p>Risk of legislative changes in the outsourcer(s) country of residence.</p> <p><i>Some jurisdictions are increasingly reacting to privacy, criminal activity and terrorism concerns with changes to and new legislation. In particular EU countries and the US have introduced a number of significant legislative changes in recent times.</i></p> <p>Risks relating to software licensing</p> <p>Software used by the outsourcer may need to be installed on local systems, or there may be unlicensed use of software by the outsourcer</p> <p>Risks from contract amendments and renegotiation</p>	
Political	<p>Risk that hosting of government information and activity offshore could be seen negatively by the public</p> <p>Risk of loss of sovereignty</p> <p>Control over government information may be lost when subject to laws/control of other countries</p>	<p>Get Minister's agreement before commencing negotiations</p> <p>Stop breaches happening</p>
Capability	<p>Risk of loss of domestic capability, including loss of organisational knowledge and strategic capability, and loss of control</p> <p><i>Local staff may be uncooperative in implementing the outsourcing project, there may be job losses, and skills to manage the outsourcing may be lost</i></p> <p>Risk of reduction in future flexibility</p> <p><i>Future options may be significantly limited</i></p> <p>Risk of loss of infrastructure in case of breakdowns</p>	<p>Regular offshore training/presence</p> <p>Ensure local capability and backup</p> <p>Effective change management</p> <p>Governance, contract and service delivery management</p>

Risk Type	Risk Description	Mitigation/Comment
	<p>Risk of service level reduction compared with local suppliers</p> <p>Risks arising from lack of cultural fit</p> <p>Can lead to difficulties in communication and performance expectations</p>	
Technology	<p>Risk of loss of connection</p> <p><i>There are only a few links between NZ and offshore locations with consequent exposure to service disruption due to natural events, or technical fault</i></p> <p>Risk of corruption of data</p> <p>Risk of service level degradation</p> <p><i>Including response times, support and reporting</i></p> <p>Risk that support infrastructure remains offshore</p>	<p>Redundancy</p> <p>Architectural design/duplication</p> <p>Understand infrastructure</p> <p>Effective governance arrangements</p>
Security	<p>Risk of non-compliance with the Security in the Government Sector (SIGS) security policy.</p> <p><i>If the information is classified, it is unlikely that it is suitable for hosting offshore</i></p> <p>Risk of non-compliance with the Protective Security Manual (PSM)</p> <p><i>In particular the impact on physical security</i></p> <p>Risk of non-compliance with other relevant NZ standards</p> <p><i>Other standards might be applied or countries don't always agree with NZ standards</i></p> <p>Risk of theft of hardware or information</p>	<p>Train offshore suppliers</p> <p>Audit offshore suppliers</p> <p>Formal governance structure</p> <p>Redundancy</p> <p>Ensure effective physical and technical security - include in contractual arrangements (Audit the implementation of these)</p> <p>Ensure consideration is given to the potential value of the information, when matched with other sources</p> <p>Business continuity planning for continued outsource operations (organisation and outsourcer) covering communication, redundancy, recovery, fault tolerance</p>

Risk Type	Risk Description	Mitigation/Comment
	<p><i>Include consideration of 'legitimate' loss to foreign country security agencies</i></p> <p>Risk of intelligence gathering</p> <p><i>The website information, and the system-produced information (such as user access logs), may be monitored or analysed by either government or business intelligence organizations, to NZ's detriment. Seemingly innocuous information may be matched with information from other sources to infer facts of greater value e.g. NZ research companies placing orders for particular items of equipment can indicate the priority areas of NZ research.</i></p> <p>Risk of external threat in the country of location</p> <p><i>Such as war, revolution, civil unrest, terrorist attack</i></p> <p>Risk of natural hazard in the country of location</p>	<p>Undertake a threat assessment</p>
<p>Fiscal</p>	<p>Risk that cost movements can be affected by exchange rate movements</p> <p>Risk of price changes by suppliers</p> <p>Risks around fixed price contracts.</p> <p>Fixed price is often balanced by varying quality in response to changing demands and conditions</p> <p>Risk of high set up and compliance costs</p> <p>Risks arising from repatriation and/or transfer to another outsourcer</p>	<p>Hedging and cost arbitrage</p> <p>Contractual controls</p> <p>Contract flexibility to reflect changing demands and conditions</p> <p>Governance, contract and service delivery management</p>

Risk Type	Risk Description	Mitigation/Comment
Economic	<p>Risk of reduced economic benefit to NZ</p> <p><i>Transferring activities offshore can reduce opportunities for NZ suppliers, although it should be noted that NZ has free trade agreements with Australia (CER) and Singapore (SNZCEP), and suppliers from these countries can therefore bid for NZ work. Additionally, NZ is negotiating free trade agreements with the following countries, therefore in the future suppliers from these countries may be bidding for NZ work: Malaysia; Pacific Islands (PACER); Chile (P3 CEP); Thailand; China.</i></p>	Cost/benefit balance
Systemic	Risk that offshore hosting could adversely impact on trust in government	<p>Education and awareness and compliance framework</p> <p>Lock down in contract</p>
Governance	<p>Risks arising from managing at arm's length</p> <p><i>There is a need to ensure that contractual and other requirements, including service reporting, are being met</i></p>	<p>Audit and compliance checks</p> <p>Contractual/legal compliance</p> <p>Reporting</p> <p>Governance structure defined in the contract</p>
Commercial	<p>Risks arising from the extra implications of private international law when negotiating a commercial contract for services</p> <p>Consideration will need to be given to the cost of foreign court legal action, if needed</p> <p>Risk of financial viability</p> <p><i>Bankruptcy, takeover, merger, further outsourcing</i></p> <p>Risk of scope creep, which may negatively affect service delivery or costs</p> <p>Maintenance of local third party (support) relationships)</p>	<p>Effective and comprehensive contracts</p> <p>Effective project and transition management</p> <p>Assessment of local relationships and formalise support arrangements</p> <p>Governance</p> <p>Roles and responsibilities definition</p> <p>Service level management & performance monitoring</p> <p>Contract management</p>

Risk Type	Risk Description	Mitigation/Comment
	<p>These may become uneconomic for local suppliers or the relationship becomes distant and unproductive</p> <p>Risk of poor or variable outsourcer performance</p> <p>Risk of contract lock-in</p> <p>This is technology-specific</p>	
Control	<p>Risk that control of data is lost</p> <p>Risk that wrong services or components are outsourced</p>	<p>Effective and comprehensive contract and processes</p> <p>Analyse internal versus outsourcer's capability,</p> <p>Assess outsourcing models</p> <p>Product/service specifications</p>
Project	<p>Risk of start-up and transition risks resulting in service interruption.</p> <p>Risk of scope creep</p> <p>Risk of organisational "pushback" and lack of co-operation</p>	<p>Project and change management</p> <p>Transition requirements specification</p> <p>Functional requirements analysis</p> <p>Governance</p>