

Vendor review questionnaire: completed example

The example used for the questionnaire is a work of fiction. Names, entities, places and incidents are used fictitiously. Any resemblance to actual events or locales or persons, living or dead, is entirely coincidental.

Vendor Name: Example Incorporated		
Section 1 - Intent	Assessment	Circle Yes/No
The beneficial owner of the vendor is from a Five Eyes country (Australia, Canada, New Zealand, UK, and US).	Result from previous internet search: Example Incorporated's parent company is located in COUNTRY A and controlled by COUNTRY A's head of state. Conclusion: Not from a Five Eyes country.	YES / NO
If YES , consider cyber security hygiene risks posed by the vendor (see the Australian Signals Directorate's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks"). If NO , go to Section 2.		
Section 2 – Vendor Jurisdiction Hazard	Assessment	Circle Yes/No
The beneficial owner of the vendor can reasonably be inferred to be controlled from a jurisdiction where there is a risk of a foreign government compelling the vendor to provide access to its private data to the government or its national security agencies (indicated by policies, legal frameworks, or public reports).	Example Incorporated's website shows that the vendor is incorporated in COUNTRY B and their parent company is based in the COUNTRY A. Internet search prompts: <ul style="list-style-type: none">COUNTRY A government data theft and accessCOUNTRY A extraterritorial laws and jurisdiction riskCOUNTRY A intelligence collection Internet search Result: nil relevant results Search of UK Overseas business risk: nil relevant risk Search of WJP Law Index: no relevant concerns	YES / NO

	<p>Conclusion: nil evidence that Example Incorporated is controlled in a jurisdiction where there is a risk of a foreign government compelling the company.</p>	
<p>The beneficial owner of the vendor can reasonably be inferred to be controlled from a jurisdiction that has been the subject of an Australian Government cyber attribution, or the Government has sanctioned the jurisdiction, or an entity within the jurisdiction, under Australian sanction law.</p>	<p>Reviewed Australian government cyber attributions announcement and sanction list</p> <p>Conclusion: Nil evidence of the COUNTRY A being sanctioned or part of malicious cyber-activities</p>	<p>YES / NO</p>
<p>The beneficial owner of the vendor can be reasonably inferred to be controlled from a jurisdiction where there is information indicating the use of economic coercion, intellectual property theft and/or technology transfer campaigns targeting Australia and/or a Five Eyes country (Australia, Canada, New Zealand, UK, and US).</p>	<p>Example Incorporated is not listed on the recent Watch list on global intellectual property protection</p> <p>Internet search prompts:</p> <ul style="list-style-type: none"> • COUNTRY A use of economic coercion • COUNTRY A government sanctioned IP theft • COUNTRY A government sanctioned technology transfer <p>Result:</p> <p>Example Incorporated - Media reporting</p> <ul style="list-style-type: none"> • Example Incorporated has strong ties to the COUNTRY A Government. COUNTRY B authorities have been concerned that Example Incorporated serves as a channel through which sophisticated COUNTRY B technology is diverted to COUNTRY A companies or the government. • JOHN DOE, COUNTRY A's head of state is the controlling shareholder and chairs the company. <p>Conclusion: There is information that Example Incorporated may be/may have been involved in technology transfer campaigns targeting COUNTRY B. As the majority shareholder is COUNTRY A's head of state, these campaigns may be government sanctioned.</p>	<p>YES / NO</p>

<p>The beneficial owner of the vendor can reasonably be inferred to be controlled from a jurisdiction where there is information indicating the vendor and/or its parent company has been sanctioned on grounds of corrupt, coercive, collusive or obstructive practices, or other integrity violations in another jurisdiction.</p>	<p>Internet search prompts:</p> <ul style="list-style-type: none"> • Example Incorporated sanctions • Example Incorporated corruption • Example Incorporated parent company • Example Global sanctions/corruptions/violations <p>Internet search:</p> <ul style="list-style-type: none"> • Example Incorporated sanctions <ul style="list-style-type: none"> ○ News Reporting: There has been more concerning reports about the company. COUNTRY B Intelligence agencies have issued warnings about Example Incorporated's work with large COUNTRY A companies that officials consider security threats. ○ Nil evidence of direct sanctions against Example Incorporated. • Example Incorporated's parent Company – Example Global <ul style="list-style-type: none"> ○ Result: JOHN DOE, COUNTRY A's head of a state is the controlling shareholder and chairs the company. • Search of United Nation's sanctions list: nil result found. <p>QWERT News: The COUNTRY B's Ministry of Commerce was asked to impose export controls on Example Global and several companies connected to it. In response, Example Global claimed that it had divested from all its investments in COUNTRY A.</p> <p>Conclusion: Sanctions were requested but not imposed on Example Global – Example Global is not listed on sanctions lists.</p>	<p>YES / NO</p>
--	--	------------------------

*If the answer is **YES** to any of the above, go to Section 4. If **NO**, go to section 3.*

Section 3 – State Ownership, Control or Influence	Assessment	Circle Yes/No
The vendor is subject to state ownership or control structures, including public information (such as information on securities websites, annual reports and business news reporting) on state shareholding of >50% or outsized state influence in corporate decision-making.	<p>Internet search prompts:</p> <ul style="list-style-type: none"> • Example Incorporated annual report • Example Incorporated ownership structure • Example Incorporated securities report • Example Incorporated business reporting • Example Incorporated shareholders <p>Result: from a recent Securities Report: JOHN DOE is the ultimate beneficial owner of Example Global. JOHN DOE is also COUNTRY A's head of state. Example Global is the majority shareholder of Example Incorporated. Example Incorporated is a wholly-owned subsidiary of Example Global. JOHN DOE exercises sole dispositive and voting control of the Common Stock and is the ultimate beneficial owner of the shares of Common Stock.</p> <p>Conclusion: Example Incorporated is subject to outsized state influence.</p>	YES / NO
There are politically exposed persons (PEPs) in senior leadership roles.	<p>Used result from the internet: JOHN DOE is COUNTRY A's head of state.</p> <p>Conclusion: There are politically affiliated persons in senior leadership roles.</p>	YES / NO
There is a special relationship between the vendor and a foreign government, providing a benefit such as special legal rights or legal status in their jurisdiction, or a privilege like unusual state funding arrangements or contracts.	<p>Internet search: Example Incorporated relationships with other countries</p> <p>Conclusion: Example Incorporated has/had significant ties with COUNTRY A, but nil evidence found that the relationship provides special benefits or privileges in terms of legal rights/funding.</p>	YES / NO

*If the answer is **YES** to any of the above, go to Section 4. If **NO**, consider cyber security hygiene risks posed by the vendor (see the Australian Signals Directorate's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks").*

Section 4 – Access and Control	Assessment	Circle Yes/No
<p>The product or service is connected, intermittently or continuously, to the internet, organisation systems or otherwise subject to third-party access.</p>	<p>Internet search: Example Incorporated (website) Result: Example Incorporated offers many products/services. Many appear to connect to the internet and systems of customers.</p> <p>Example Incorporated AI product ‘AI123’ showcase on website: Showcase of using Example Incorporated’s newest AI product ‘AI123’ to enable physical security: Example Incorporated’s AI123 product uses a remote access management system to monitor physical assets that can integrate with the customer’s/host’s information systems Conclusion: AI123 is connected to internet and organisation systems</p>	<p>YES / NO</p>
<p>The vendor has excessive or unusual data collection practices or there are indicators the vendor is sharing its data with a foreign military organisation or intelligence/security service (such as through military-civilian industrial cooperation arrangements).</p>	<p>Internet search prompts:</p> <ul style="list-style-type: none"> • Example Incorporated data collection • Example Incorporated data sharing • Example Incorporated military data • Example Incorporated intelligence sharing <p>Internet search: Example Incorporated Data collection</p> <p>Result: A COUNTRY B government investigation into Example Incorporated found that:</p> <ul style="list-style-type: none"> • Example Incorporated maintains relationships with COUNTRY B blacklisted entities. • Multiple COUNTRY B companies that develop and sell export-controlled technology and products maintain extensive commercial relationships with Example Global and its subsidiaries, which leaves COUNTRY B companies susceptible to COUNTRY A directed IP theft. • Example Incorporated-linked companies and executives are affiliated with COUNTRY A engineers who stole millions of dollars of COUNTRY B military-funded research from the UNIVERSITY 	<p>YES / NO</p>

	<p>OF COUNTRY B in order to create a new COUNTRY A government laboratory in COUNTRY A.</p> <p>Conclusion: there are indicators that Example Incorporated is sharing its data with a foreign military organisation or intelligence/security service.</p>	
--	--	--

*If the answer is **YES** to any of the above, **conduct a vendor FOCI risk assessment**. If **NO**, consider cyber security hygiene risks posed by the vendor (see the Australian Signals Directorate's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks") and risks associated with disruption or suspension of service.*

Preliminary Assessment: Before commencing in any contractual agreement, a vendor FOCI risk assessment should form part of our procurement due diligence process.