NSW ICT Short Form Contract Review

AIIA Feedback to DFSI on new Short Form ICT Agreement

25 January 2018

GPO Box 573
Canberra ACT 2601

T +61 2 6281 9402
E s.roche@aiia.com.au
W www.aiia.com.au

About AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. AIIA is a not-for-profit organisation that has, since 1978, pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment and drive Australia's social and economic prosperity.

AIIA does this by: providing a strong voice on policy priorities and a sense of community through events and education; enabling a dynamic network of collaboration and inspiration; and curating compelling content and relevant information.

AIIA's members range from start-ups and the incubators that house them, to small and medium-sized businesses including many 'scale-ups' and large Australian and global organisations. We represent global brands including Apple, Adobe, CISCO, Deloitte, DXC, Gartner, Google, IBM, Infosys, KPMG, Lenovo, Microsoft and Oracle; international companies including Optus and Telstra; national companies including Ajilon, Data#3, SMS Management and Technology and Technology One. While AIIA's members represent around two-thirds of the technology revenues in Australia, more than 90% of our members are SMEs.

Our national board represents the diversity of the digital economy; more detailed information is available on our web site.

Introduction

AIIA is grateful for the opportunity to respond to the consultation process on the review of the Short Form Contract.

Our Submission recommends the Department of Finance, Services and Innovation (DDSI) consider the following collated feedback on the four documents that have been released for feedback under the proposed simple ICT agreement.

Overview

The AIIA is supportive of developing the Short Form Procure IT contact for low risk, low value procurements. Overall, members are supportive of increasing the limit available to purchase to $500k, increasing the usefulness and adoption of a Short Form contract. We are concerned however, that this process appears to apply even more restrictive provisions than the current long form Procure IT contract.

In summary AIIA is:

- supportive of the proposed Short Form ICT Agreement structure.
- supportive of the plain language drafting and layout proposed.
- supportive of the limited indemnities. However, the way different types of data are addressed would benefit from more consideration and there are grave concerns about the liability and other clauses that are discussed further below.
- AIIA has no comments on the renewal or service credit issues. We don't have any other suggestions on these issues.

Core Terms - Short Form ICT Agreement

On the front cover, under the Notes to Customers at the third dot-point, we note DFSI intend to exclude any solutions that involve personal information going offshore.

Increasingly, cloud solutions and global support arrangements will involve third party handling of data, which will require agencies to assess risk.

We are not aware of any NSW law or policy that prohibits the transfer of data offshore, only that such transfers require risk assessment to comply with NO-12 and the NSW Government Cloud Policy. The necessity of incrementally extending a risk assessment to consider issues around data being transferred offshore, such as the form of that data, the types of data being transferred, classification of that data and security measures in place, is not a good foundation for a rigid exclusion of otherwise low risk, low value IT services engagements from the scope of this short form ICT Agreement.

In addition, this position is inconsistent with Clause 8, with many vendors providing global f maintenance and support services to meet client service requirements.

It is also inconsistent with Clause 11 of the "aaS" Solution Requirements document, which looks to have the service evolve over time.

Overall members strongly believe that given the expected higher use with the increased threshold, and as simple cloud solutions and IT services become less expensive with automation and other innovations, this Short Form ICT Agreement should be consistent with the long form Procure IT contract and allow offshoring with consent.

Clause 1. Core Terms

In line with the effort to achieve plain language drafting, please number subparagraphs in these clauses, for easy reference.

As DFSI will update the contract from time to time, please number the versions, to enable appropriate r version control.

Clause 3. Performance

Second dot point – working with nominated partners: It is unreasonable to have this as broadly stated as it is. An acceptable position is to exclude competitors or extend the provision to incorporate "and such partners directly enter deeds of confidentiality with you".

Fourth dot point – reasonable directions: Suppliers will only agree to this, if the reasonable direction does not involve a scope creep, or material change to the cost in providing the solution. If there is a material change in the cost, suppliers should be reimbursed costs of compliance.

Clause 4. User materials

It is recommended that the term "solution" is replaced with the term "deliverables" as this accounts for a broader range of products and services that may be purchased. The term "solution" may not be accurate in many cases. Such a change should be replicated in the As a Service terms and Professional Services terms.

Clause 6 – Confidential Information

The AIIA recommends reinstating the general exclusion of information in the public domain (through no fault of any party) from the definition of Confidential Information. As noted by the High Court, failure to include this exception may risk the Clause being found to be an unenforceable restraint of trade,[1] especially if information can be designated as confidential by the customer.

We also recommend amending the first row to require that each party that discloses confidential information must also ensure the third party recipient of the information must also hold the information

[1] See *Maggbury Pty Ltd v Hafele Australia Pty Ltd* [2001] HCA 70.

confidential. Disclosure to a subcontractor would under current drafting would waive confidentiality requirements.

Clause 7. Customer Data

The expanded definition of "Customer Data" must be limited to only Government provided or created information.

We strongly recommend that dot points 1 and 3 are deleted from the definition of Customer Data and the definition in dot point 4 narrowed to specific non-public and relevant information about the customer's operations.

While it is fine to designate customer data as confidential, not all confidential information is necessarily customer data, and not all information processed or stored by a supplier will be customer data. As the clause stands, anonymous metadata generated by use of a solution as part of acceptance testing by a supplier is included as customer data that becomes confidential and owned by the customer (clause 7, row 3) even if the parties have agreed the supplier should own it as the supplier's pre-existing materials (clause 10). Members will not agree to this. If this is not amended, many suppliers will be unable to use the Short Form ICT Agreement and/or the scope of services offerings that can be transacted under this contract will be greatly reduced.

For similar reasons, the fourth row should be deleted. It is superfluous in that clause 10 deals with IP ownership, the fifth row already provides the relevant authorisation or licence to use data and the "non-transferable" restriction conflicts with any subcontracting pursuant to clause 5.

The 2nd and 3rd dot points of the last row of that section should be amended to align with the Privacy Laws and NSW Government Cloud Policies. Neither NSW law nor NSW cloud policy prevents data analytics of information that cannot be used to identify a person (i.e. because it is not personal information). These provisions would preclude suppliers from using redacted analytics to improve their products and services and they conflict with the improvement of the service in clause 11 of the "aaS" Solution Requirements.

The AIIA also recommends Customers expressly indicating or specifying at the ordering stage, what if any Customer Data they would expect to be returned so that the data can be collected, stored and managed accordingly.

Clause 8. Privacy

We believe that the need for an outright prohibition of offshoring personal information is entirely unnecessary and will defeat the point of increasing the usage threshold to $500k.

The majority of "aaS" solutions will not be able to use this contract, as they rely on cloud platforms, support systems based overseas, or hybrid solutions with cloud-based analytics.

Clause 9. Security

We note that the security breach requirements are inconsistent with the new data breach reporting requirements. If requirements are not aligned, suppliers may need to provide bespoke security monitoring and reporting beyond what is required by law, or limit the service offerings available to be transacted under this short form ICT Agreement.

For example, the Security breach definition would have to be limited to Personal Information only. Measures adopted must be reasonable, given that increased security will almost always reduce accessibility, latency and usability. The obligation to notify within a 48hour timeframe is also extremely short, even less than the obligations under the European GDPR requirements.

Also, we observe that the final row does not adequately address the scenario where an agency reasonably (but erroneously) believes there is a security breach. It would not be possible for suppliers to provide "summary measures … to mitigate the impact" where there is no impact. Our members recommend the response by suppliers be to "conduct a reasonable investigation and report to the customer", with the reports and data set out in dot points provided as examples of what the

Government would regard to be a reasonable investigation or report in the event of a security breach, whereas measures to mitigate a security breach should be developed jointly rather than provided by the supplier alone.

We would further note that measures undertaken by vendors to mitigate impact may be commercial in confidence and/or an obligation to provide such detail may undermine the overall integrity of the vendor's security operations.

Clause 10. Intellectual Property

Fourth row – new materials licence: For aaS solutions, this licence must be limited to the term of the agreement. The licence does not continue perpetually after the arrangement. This is a core concept of "aaS" term licensing models.

Clause 11. Transparency

Delete general right to inspect records. This would need to be limited to an annual audit only, the scope of which the vendor and customer to agree on prior; in order for this to be manageable across all customers.

Clause 14. Indemnity

The indemnity should be limited to direct losses. It should not be a full indemnity for all direct and indirect loss. This is an unacceptable position for suppliers.

To make it clear that the indemnity is limited to any infringement that arises as a result of the customer's use of the vendor's products/services. the second half of sentence should be replaced with "…brought by a third party in respect of any infringement or alleged infringement of a third party's intellectual property rights because of the use of your products".

Clause 15. Liability

The AIIA strongly recommends adopting a liability position closer to that of the previous short form ICT contract, which featured:

- an exclusion of all consequential loss (including under the indemnity); and
- liability for breach of privacy falling within the general liability cap.

The exclusion of consequential loss is a standard provision in the industry, is a common condition in insurance policies and a fair and reasonable position for low risk, low value, business-as-usual services engagements. A capped liability for privacy breaches is also fair and reasonable taking into account the historical quantum of liability from Australian privacy breaches and the fact government agencies must still conduct risk assessments in relation to privacy. Indeed, retaining an unlimited liability for privacy breaches will encourage some agencies to rely on that as the sole risk mitigation for privacy issues, even though the more laborious risk assessment process is more effective and the required approach under NSW government policies.

We recommend the liability cap be limited to "two times the fees set out in the agreement", to allow a reasonable, proportionate and industry standard limitation to a supplier's exposure. Less proportionate caps (when compared with the potential benefit of the contract), such as an arbitrary liability cap imposes a "risk tax" that will discourage using this short form ICT Agreement for very low value IT services engagements.

Clause 16. Termination for Cause

Given the gravity, the trigger for such termination should be limited to "material breaches" of the Agreement. It is an unacceptable position allowing termination for minor breaches ie., SLA breaches.

The vendor should be able to specify the termination amount due as there may be various amounts that they will be unable to recoup because of early termination.

Clause 17. Early Termination

This clause may work for professional services and the procurement of hardware. Most "aaS" or other ICT procurements involve amortised hardware or other costs over the term of the Agreement, that early termination charges seek to recoup. This clause needs to make reference to any applicable early termination charges, or at the very least, reimbursement of reasonable stranded or amortised costs. The purchase of software maintenance using this approach, will not be permitted by software vendors who following normal accounting practices, will be unable to recognise the revenue.

Missing Clauses

The Agreement needs to provide for force majeure.

If telecommunications services are intended to be procured under this, there needs to be a migration clause created (in line with the migration clause in the current Telco Module of Procure ITv3.2.. We acknowledge that the intent may be to incorporate this in a specific solution requirement yet to be released.

A section on customer inputs/dependencies should also be included.

Solution Requirements – Professional Services

Clause 2 | Your representations | Row 2

The statement is very broad and should be specific to representations in writing, or other specific modes of communication.

Clause 3 | Performance | Bullet 2

Working cooperatively is a broad expression and may lead to scope creep and add-on costs to the service provider and needs to be narrowed down.

Clause 3 | Performance | Bullet 3

Suppliers act in accordance to the laws applicable to them as a professional services provider. The clients will need to advise the laws and regulations which the client needs to comply with so that the

Clause 4 | User Material | Row 1

Reference to 'all' user material is a broad statement and can be referenced to a certain level of training or referenced to further detail specified in the statement of work.

Clause 5 | Subcontracting | Row 1

This is expected to refer to third party service provider subcontracting firms only. Related organisational entities e.g. overseas supplier entities and independent contractors should be excluded.

Clause 6 | Confidential Information | Row 3

Disclosing or making information public should be post mutual discussions and agreement between parties and an opportunity for the service provider to review for the information is made public.

Clause 7 | Customer Data | Row 4

The license for data should be transferrable to any subcontractor for the purposes of the engagement and they will be required to comply with the same confidentiality requirements.

Clause 14 | Indemnity

For the purposes of 'conduct of claims'

- the service provider should have the ability to run the process;
- the client (Agency) should be liable to mitigate their losses (the service provider should not be liable for any additional losses which the client incurs).

Clause 15 | Liability | Row 1

This should include some form of culpability e.g. misuse or misappropriation of confidential or personal information

Clause 16 | Termination for Cause

Amortised Costs for the days when service is provided until the termination of service will be payable.

Approach to Renewal / Re-signing arrangements

If the relationship with the existing provider is progressing well and there is confidence in leadership level, an automatic renewal could be preferred option.

Automated renewals may include / require

- discounts based on productivity improvements
- A separate approval cap / limit to be defined
- some safeguards to be put in place to ensure that required due diligence is carried out before renewals
- final accountability lies with leadership

Solution Requirements – "aaS"

Clause 4. Outcome or business need

This clause might be appropriate for professional services, but is not appropriate for specifically scoped, ICT solutions. It can remain as a mere acknowledgement, but Suppliers should not be held in breach, if the solution does not meet that business need or outcome. It should be measured against the solution as set out in this short form ICT Agreement.

Clause 6

The mechanics of the service level credit regime are overly prescriptive and may be too rigid for the way vendors may issue the credits (eg it may not necessarily be against the invoice).

Clause 7

This section should be removed. Generally, As a Service services are not bespoke and not tailored towards any one specific customer's needs. The customer needs to be responsible for completing their due diligence to ensure that the product adequately meets their needs.

Clause 11. Changes to the aaS Solution

The first dot point is inconsistent with the third dot point.

Whilst an ICT solution can be updated or replaced over time –this might have a cost impact. We acknowledge this clause may be appropriate for software version updates, it is drafted so broadly, that it could apply to updates of whole platforms. There is no option, for individual vendors to opt-in or express the extent of what may or may not be offered as a 'free' enhancement and any associated limitations.

Suppliers who have roadmaps may be happy to provide these to NSW Government, but if those changes are accepted, the Govt will need to agree a contract variation with the change in scope and pricing that it would entail.

To provide an example – if you as a consumer, realised that Apple has released a new iPhone 2 months after purchasing your current Iphone, would you expect them to upgrade your Iphone during the term of the contract for no additional cost? The logic must be applied here for commercial ICT solutions.

Whilst the drafting may have been performed with the best of intentions, it does not stand up to commercial scrutiny from an operational perspective.

Clause 12. Insurance

The long form Procure IT and the existing short form agreement allows suppliers to self-insure. It is not clear from this if suppliers may self-insure for these specified clauses. We recommend that this clause be amended to acknowledge that suppliers may self-insure for these clauses, with customer consent and incorporate "in the annual aggregate" for product liability.

Clause 13

Third point should be changed to "…you must ensure that the as-a-service [deliverable] shall not materially degrade from the Service Description set out above in relation to the performance, functionality, security and availability of the as-a service".

Summary

While AIIA strongly supports the current review of the t Short form Agreement (indeed, we believe it is well overdue), there are a number of key concerns (outlined above) that we highly recommend are addressed before the Contract is released for general use.

As noted in our response key concerns related to the Customer Service definition, changes to solutions, failure to exclude consequential loss, IP and no allowance for early termination charges are not commercially acceptable to many of our members and, as a result, they will not use the Agreement as drafted. This effectively defeats its purpose and undermines streamlining of current procurement arrangements.

As we have always indicated, AIIA is very pleased to come to the table and discuss/negotiate contract terms to achieve mutually beneficial outcomes. We make this offer again in this case – with the shared objective of having a practical, workable Contract for ICT vendors.