Marketplace

Tier 1 Security Assurance Terms

SaaS Channel, Managed Services Channel, Enterprise Software Channel, Digital Identity Channel – All Marketplace Catalogues

For Providers Seeking a Tier 1 Security Assurance and Risk Rating

Background

Providers of Services in the SaaS Channel, the Managed Services Channel, Enterprise Software Channel and the Digital Identity Channel may apply to the Government Chief Digital Officer (**GCDO**) at the Department of Internal Affairs (**we**, **our**, **us**) for a specific tier of security assurance. There are three tiers. Tier 1 (Design and Control Effectiveness) is the highest tier, providing the highest level of security assurance that a provider can obtain for a Services Listing in the Marketplace. It provides the greatest level of support to Purchasing Agencies' security risk and assurance processes and decisions. That, in turn, is likely to foster greater levels of trust and confidence in the Tier 1-rated Service and may result in greater uptake. To obtain a Tier 1 Security Assurance and Risk Rating, Providers need to provide additional information and receive information security certification from the GCDO.

When applying for this rating, Providers need to agree to these Tier 1 Security Assurance Terms. They are not negotiable. When agreed to, they form part of the Channel Terms for the SaaS Channel, Managed Services Channel, Enterprise Software Channel or Digital Identity Channel (as applicable, depending on the Channel in which the relevant Service resides). The Channel Terms are part of the Collaborative Marketplace Agreement between the Provider and the Department of Internal Affairs.

Contents

1. Provision of information and access

1.1 Without limiting clause 3 (Membership) of Part 1 (General Terms) of the Agreement, you must provide us in a timely manner and at your cost with access to all information, documentation, reports, tools and people that we may reasonably require to inform:

(a) our consideration of your application for a Tier 1 Security Assurance and Risk Rating; and, if granted

(b) our subsequent periodic re-certification of the Service for which you have obtained the Tier 1 Security Assurance and Risk Rating (which, given New Zealand Information Security Manual requirements, you can expect us to do at least once every 3 years),

including if required a report from an independent auditor.

You must provide us with the information and other things we need to assess your application or for our periodic re-certification of your Service.

1.2 If you do not comply with clause 1.1:

(a) we may inform you by notice in writing that, if you do not comply within a specified timeframe:

(i) we may (where relevant) decline your application without further consideration; and

(ii) if you have a Services Listing for a Service that requires a Tier 1 Security Assurance and Risk Rating to remain within the Marketplace,[1] we may suspend or terminate the Services Listing; and

(b) if you do not comply with the timeframe specified in our written notice, we may:

(i) decline your application (where relevant) without further consideration and inform you accordingly; and

(ii) where clause 1.2(a)(ii) applies, suspend or terminate the Services Listing.

2. Processing of applications

2.1 You agree that we may, acting reasonably, process, prioritise or decline applications for Tier 1 Security Assurance and Risk Ratings, based on our understanding of agency demand and our resourcing.

We may need to process, prioritise or decline applications based on demand and resourcing.

3. Grant of Tier 1 Security Assurance and Risk Rating

3.1 We may grant, or continue the grant of (following a re-certification process), a Tier 1 Security Assurance and Risk Rating, either with or

[1] Your Service may, for example, have been listed at tier 2 but, after a certain period, need to obtain a Tier 1 Security Assurance and Risk Rating to remain in the Marketplace, usually as notified to you in a notice of procurement on the Government Electronic Tenders Service or on the Marketplace or during initial onboarding.

without conditions, if you and the Service meet our requirements for such a rating. Any conditions must be reasonable in the circumstances and they must relate to the Tier 1 Service and government security requirements existing as at the date of your application for the rating or the date of our re-certification (as applicable).

We may grant your application or re-certify the Service with conditions (which must be reasonable) and we may grant the application or re-certify the Service wholly or in part.

3.2 We reserve the right to grant, or to continue the grant of, a Tier 1 Security Assurance and Risk Rating to the entirety of the relevant Service or only to parts of it. If any part of the Tier 1 Service is not covered by the rating, you must make this clear in your Services Listing.

4. Continuance of Tier 1 Security Assurance and Risk Rating

Your continued enjoyment of any Tier 1 rating we grant is subject to certain conditions being met.

4.1 If we grant you a Tier 1 Security Assurance and Risk Rating, the continuance of that rating within the Marketplace for the relevant Tier 1 Service is subject to the following conditions:

(a) your compliance with these Tier 1 Security Assurance Terms;

(b) your responding appropriately to any security breach or loss of Purchasing Agency Data or Confidential Information that occurs;

(c) your (and any relevant Subcontractors) having in place adequate internal controls for security, availability, processing integrity, confidentiality and privacy in relation to the Tier 1 Services provided, as may be evidenced by an independent assurance report provided in accordance with clause 6.1; and

(d) your obtaining periodic re-certification from us as referred to in clause 1.1(b),

each as determined by us in our sole discretion (acting reasonably).

If you don’t continue to meet the conditions mentioned above, we may downgrade your assurance rating, but we’ll discuss this with you before doing so.

4.2 Subject to clause 4.3, if, at any time, we consider (acting reasonably) that one or more conditions in clause 4.1 is not met, we may by written notice to you:

(a) elect to downgrade your security assurance tier for the affected Tier 1 Service or, where clause 1.2(a)(ii) applies, suspend or terminate the Services Listing; and

(b) amend the relevant Services Listing accordingly or require you to do so within a reasonable timeframe we specify or, where clause 1.2(a)(ii) applies, remove the Services Listing.

4.3 Before downgrading your security assurance tier or suspending or terminating the Services Listing under clause 4.2, we will give you a reasonable opportunity:

(a) to comment on our reasons for proposing to do so; and

(b) if we consider it appropriate, to rectify the issues or problems at your cost within a reasonable timeframe we specify.

4.4 If we give you an opportunity to recitfy issues or problems under clause 4.3(b) and you do so to our reasonable satisfaction within the timeframe we specify, we will not downgrade your security assurance tier or suspend or terminate the Services Listing for the affected Tier 1 Service under clause 4.2.

5. Security governance meetings

5.1 You will attend security governance meetings with us as we may reasonably request and at the locations or by the means that we may reasonably request. If you wish to participate via video-conferencing or similar means, you may ask to do so and we will not unreasonably deny your request.

You may need to participate in security governance meetings.

5.2 When you attend such a meeting, you will ensure you are represented by Personnel who have the relevant knowledge, experience, involvement and authority having regard to the purpose of the meeting.

6. Audit and assurance

6.1 Independent assurance

(a) You agree to undertake an annual independent assurance review of the design and operating effectiveness of your key internal controls for security, availability, processing integrity, confidentiality and privacy in relation to those of your Services Listings for which you have sought and obtained a Tier 1 Security Assurance and Risk Rating.

You need to have an external and independent reviewer undertake annual assurance reviews.

(b) The review must be performed by an external and independent reviewer and shall assess your controls against criteria relevant to the Services.

(c) The review scope must extend to any controls that you (or any relevant Subcontractor) have in place in respect of any functions or services performed by relevant Subcontractors. The scope of the review must be commensurate with the complexity of, and risks related to, the Services. The review should follow, or be equivalent in approach to the approach in, the American Institute of CPAs SOC 2 Type 2 *Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*.

(d) You will provide a written report to the GCDO detailing the findings of the review promptly following completion of the review and you will be responsible for the costs of the review.

6.2 Right to audit

If we are not satisfied with the information received from any independent assurance process under clause 6.1 or consider that there is a pressing need for an audit where it would not be practicable to wait for an audit to be carried out under clause 6.1 (or

In certain circumstances we may undertake our own audit. If we do, you will need to co-operate.

to wait for results of any such audit to be received), we may, from time to time, carry out an audit for the purpose of:

(a) reviewing your operational integrity and your compliance with, and/or ability to perform, any of your obligations under, or in connection with, the Agreement and/or any or all Agency Purchase Agreements; or

(b) confirming the accuracy of any invoice you have rendered to any Purchasing Agency.

6.3 Audit requirements

If we conduct an audit under this clause 6:

(a) it will be conducted during Business Days, during normal business hours, and following 10 Business Days' written notice to you;

(b) it may, at our option, be undertaken by our Personnel, or an independent expert approved by you (such approval not to be unreasonably withheld) (**Auditor**), with the Auditor to be under a duty of confidentiality;

(c) we will comply (and will take reasonable steps to ensure any Auditor complies) with your reasonable requirements for the purpose of protecting the security and safety of personnel, information and premises;

(d) we will use reasonable endeavours to minimise (including taking reasonable steps to ensure any Auditor minimises) any disruption to your business during the course of the audit;

(e) you must co-operate in a timely manner in respect of any audit; and

(f) you must promptly provide:

(i) access and assistance to us in respect of any audit (including access to you, your Personnel, facilities, systems, records and resources used in the provision of the Services); and

(ii) any explanations, information and documentation that we may reasonably require in relation to the audit.

6.4 Cost of audit

We will be responsible for our costs and you will be responsible for your costs in relation to any audit undertaken in accordance with this clause 6, unless the audit reveals a material breach by you of this Agreement and/or any Agency Purchase Agreement, in which case you will reimburse us for our actual and reasonable costs in carrying out any audit.

6.5 Outcome of audit

Without limiting any other provision of this Agreement or rights or remedies available to us or any Purchasing Agency, if an audit reveals a failure by you to comply with this Agreement or any Agency Purchase Agreement, or any inaccurate information given or invoice rendered to a Purchasing Agency, you will prompty remedy such failure or inaccuracy or (as the context requires) resolve such findings, at your own cost and to our reasonable satisfaction.

7. Business continuity planning

7.1 Your obligation

You need to implement and maintain business continuity arrangements, including BC/DR Plans, and test the plans periodically in accordance with this clause.

You will:

(a) implement and maintain at all times adequate business continuity and disaster recovery arrangements in respect of your own business in accordance with Good Industry Practice; and

(b) maintain documented and tested business continuity and disaster recovery plans in respect of the Services for which you have a Tier 1 Security Assurance and Risk Rating (the **BC/DR Plans**) and will provide an up-to-date copy of such plans to us within 5 Business Days of a written request.

7.2 Risk Mitigation

You need to try to prevent or mitigate events that pose business continuity risks.

Without limiting clause 7.1, you shall:

(a) use all reasonable endeavours to prevent or mitigate any Trigger Event (as defined in clause 7.2(b)) that may affect your ability to provide the Tier 1 Services under this Agreement.

(b) For the purposes of this clause 7.2, a **Trigger Event** means:

(i) a disaster or crisis situation (including any financial crisis or stress impacting on the provision of the Tier 1 Services); or

(ii) a situation or event where your business infrastructure or resources are destroyed, damaged or their use or availability is otherwise interrupted.

7.3 Contents of plans

Your BC/DR Plans need to cover the topics we list here.

(a) The BC/DR Plans will:

(i) provide an end-to-end business continuity and disaster recovery strategy to enable you to resume the supply of the Tier 1 Services to a pre-specified level/time, possibly from an alternative location, or using alternative resources or staff, to limit any adverse impact on the delivery of the Tier 1 Services; and

(ii) describe how technical capabilities and alternate location arrangements support business continuity.

(b) They will (where relevant):

(i) address resiliency, business continuation, disaster recovery, and crisis management issues in response to a Trigger Event such as:

(A) the technical and management infrastructure;

(B) the processes required to operate the Tier 1 Services;

(C) the people required to operate the Tier 1 Services;

(D) any third-party suppliers used in providing the Tier 1 Services;

(E) events mitigated against, e.g., timeframes to restore to various levels of capability;

(F) measures you have taken to minimise the risk of your business being affected by a Trigger Event; and

(G) actions you have taken to evidence the robustness of your business continuity plans;

(ii) include restoration of key systems capability in the event of loss of key site, Personnel, and technology infrastructure;

(iii) include the location of recovery site(s) for each of your locations at or from which the Tier 1 Services are provided and/or where Purchasing Agency Data are stored;

(iv) provide for steps you will take to mitigate any material disruption to the provision of Tier 1 Services;

(v) be designed to recover business operations as soon as reasonably practicable in the circumstances after a Trigger Event; and

(vi) provide for the ongoing testing of such BC/DR Plans.

7.4 Plans review

(a) Within 30 days of your clicking to accept these Tier 1 Security Assurance Terms, and from time to time at our request, you will submit the BC/DR Plans to us for review.

There are times when you'll need to provide your BC/DR Plans to us for review.

(b) We may request reasonable amendments to the BC/DR Plans following any review undertaken in accordance with clause 7.4(a) above.

(c) You agree to provide such additional information as may be reasonably necessary to allow each Purchasing Agency to develop its own business continuity and disaster recovery plan or plans to work in concert with the BC/DR Plans at no additional cost to any Purchasing Agency.

(d) To avoid doubt, the BC/DR Plans, and any information provided to us and any Purchasing Agency in connection with the BC/DR Plans under this clause 7.4 shall be considered and treated as your Confidential Information under the Agreement.

7.5 Implementation

Upon the occurrence of one or more Trigger Events, you shall inform us in writing as to whether you are implementing the relevant portion or portions of the BC/DR Plans and, if not, why not.

If a Trigger Event occurs, you need to tell us whether you're implementing your BC/DR Plans.

7.6 Testing

(a) You shall review, test and, where appropriate, update the procedures set out in the BC/DR Plans no less than once per calendar year. You must inform us of the initial results of any testing within 30 days of the completion of the test. A final report will be issued to us no later than 60 days from the completion of the test. You will inform us and Purchasing Agencies of the timing and nature of such testing to enable us and Purchasing Agencies to manage any impact of such testing and to co-ordinate the testing of each Purchasing Agency's own plans, where appropriate.

You need to test your BC/DR Plans no less than once a year and inform us of the testing results.

(b) If we consider, acting reasonably, that you may not be fully compliant with your obligations under this clause, we may appoint an auditor to audit such compliance in accordance with clause 6.2 above.

7.7 General

Within 30 days of your clicking to accept these Tier 1 Security Assurance Terms, you shall appoint a crisis manager and shall notify us of such appointment. The role of the crisis manager shall be to act as the key point of contact between us and you in the event of any disaster or crisis affecting any of the Tier 1 Services and/or the operations of any Purchasing Agency. You shall ensure that we have 24/7 contact details for the crisis manager (or his or her successor or alternate appointed from time to time).

You need to appoint a crisis manager that we can liaise with in the event of a disaster or crisis.

8. Security risk and incident reporting

8.1 If you become aware or suspect that:

(a) there is a material vulnerability in any of your Tier 1 Services;

(b) any unauthorised person has obtained access to the technology systems you use for the Tier 1 Services or any Confidential Information or Purchasing Agency Data;

(c) any person has used any Confidential Information or Purchasing Agency Data for purposes not authorised or permitted by the Agreement or an Agency Purchase Agreement (as applicable); or

(d) any other unauthorised access or other incident (including compromise or unauthorised exfiltration of Purchasing Agency Data) has occurred that threatens the security or integrity of the Tier 1 Services or any Confidential Information or Purchasing Agency Data,

the following steps shall be taken, as applicable:

(e) you will notify us and Purchasing Agencies as soon as possible (unless only one or a small number of Purchasing Agencies are affected in which case you may elect to inform only that one or those Purchasing Agencies);

(f) where the incident concerns unauthorised access, promptly take such steps as are reasonably available to you to:

(i) identify the person or persons who have gained access; and

(ii) provide us (or the relevant Purchasing Agencies) with such information to assist with investigation of the incident as we (or the relevant Purchasing Agencies) may reasonably request; and

(g) take all reasonable steps to stop such unauthorised access or incident and prevent its reoccurrence.

If you become aware of or suspect a security risk, you need to take the steps specified in this clause.

9. Technical risk register

9.1 You will:

(a) maintain and keep current a technical risk register (the **Risk Register**) that identifies:

(i) risks to the security and availability of the Tier 1 Services; and

(ii) for each risk:

(A) the nature and underlying cause of the risk;

(B) the impact of the risk should it materialise; and

You need to maintain a technical risk register and provide a copy to us if we ask for it.

(C) the controls in place to mitigate the risk; and

(b) provide a copy of the Risk Register to us promptly upon being requested to do so.

10. Information sharing

10.1 Despite any other provision in the Agreement, you agree we may share information obtained:

(a) under clause 8 (Security risk and incident reporting), with the impacted Purchasing Agency or Agencies; and

(b) under clause 9 (Technical risk register), with any Purchasing Agency,

provided we ensure that the Purchasing Agency or Agencies are aware that the information is Confidential Information and must not be shared with other agencies or organisations without your written consent.

We may share security incident and risk register information with certain Purchasing Agencies, as long as we make it clear that it's confidential.

11. Change

11.1 If you are proposing to make any Change (as defined in clause 13) to a Tier 1 Service, you must consider:

(a) whether the Change will or could adversely affect the security or other controls in place for the Service;

(b) whether the Change will or could affect your compliance with applicable standards (e.g., coding standards);

(c) whether, given the nature of the Change, additional security or other controls are required to:

(i) secure the Service;

(ii) maintain the confidentiality, integrity and availability of the Purchasing Agency's Confidential Information;

(iii) protect the Purchasing Agency's Confidential Information from unauthorised use or access; or

(iv) otherwise meet our requirements (including any particular controls) for a Tier 1 Security Assurance and Risk Rating.

Changes to a Tier 1 Service can affect its security risk profile and our certification, and so you need to consider potential impacts before making certain kinds of changes and tell us about the potential impacts.

11.2 Having considered the matters in clause 11.1, you must:

(a) prepare a written statement (an **Impact Statement**) that:

(i) describes the Change and its impact on the matters specified in clause 11.1, using any reasonable template we may provide to you for this purpose and including any other information required by the template; and

When you provide an Impact Statement to us, you also need to tell us whether you're seeking an extension or amendment of your Tier 1 Security Assurance and Risk Rating.

(ii) states whether you are seeking an extension or amendment of your existing Tier 1 Security Assurance and Risk Rating to cover the Change; and

(b) provide the Impact Statement to us as soon as practicable and in any event 30 days before the Change is implemented. Clauses 1 to 3 apply to any request for an extension or amendment of your existing Tier 1 Security Assurance and Risk Rating to cover the Change.

11.3 Regardless of whether you are seeking an extension or amendment of your existing Tier 1 Security Assurance and Risk Rating to cover the Change, you must not implement the Change before either:

(a) obtaining our written confirmation that the Change may be included within your Tier 1 Security Assurance and Risk Rating; or

(b) if you are not seeking such confirmation or you wish to implement the Change before obtaining such confirmation, amending your Services Listing to note that the Change does not currently fall within your Tier 1 Security Assurance and Risk Rating and informing all Purchasing Agencies of this fact at least 30 days before the Change is implemented.

You can't implement a Change before either we confirm it's covered by your Tier 1 rating or you comply with the transparency requirements stated here.

11.4 If:

(a) you are not seeking our written confirmation that the Change may be included within your Tier 1 Security Assurance and Risk Rating, or you implement the Change before obtaining such confirmation; and

(b) we consider that the Change causes or will cause one or more of the conditions in clause 4.1(a)-(c) to no longer be met in relation to what is already covered by that rating (for example, if hosting were being shifted to an unsafe country),

we may exercise our rights in clause 4.2, subject to our compliance with clauses 4.3-4.4.

If you implement a Change without our confirmation that your Tier 1 rating extends to it and the Change jeopardises your existing Tier 1 rating (in relation to what it covers), we may exercise our tiering downgrade and related rights in clause 4.

12. No limitation and precedence

12.1 To avoid doubt, these Tier 1 Security Assurance Terms do not limit security-related or other obligations you owe to:

(a) us under the Collaborative Marketplace Agreement (including any applicable Channel Terms); or

(b) Purchasing Agencies under their Agency Purchase Agreements.

These Tier 1 Security Assurance Terms don't limit obligations you have elsewhere.

12.2 If there is any conflict between these Tier 1 Security Assurance Terms and other terms of the Collaborative Marketplace Agreement, these Tier 1 Security Assurance Terms prevail to the extent of the inconsistency.

13. Definitions and interpretation

13.1 These Tier 1 Security Assurance Terms incorporate all relevant definitions included in the General Terms in Part 1 of the Marketplace Agreement. In addition, for the purposes of these Tier 1 Security Assurance Terms:

These defined terms have the particular meanings given to them.

Agreement means the Collaborative Marketplace Agreement (also known as the Marketplace Agreement), of which these Tier 1 Security Assurance Terms form a part when accepted by a service provider that applies for a Tier 1 Security Assurance and Risk Rating;

Business Day means any day other than a Saturday, a Sunday or a public holiday (as defined in the Holidays Act 2003) in Wellington, New Zealand;

Change means any of the following kinds of changes to or affecting a Tier 1 Service:

(a) changes to the Service's code base that materially impact the design of the solution and the way Purchasing Agency Data are accessed, stored or processed (excluding, to avoid doubt, everyday patches, bug fixes, cosmetic changes and the like);

(b) features (including new features) that materially change the way Purchasing Agency Data are accessed, stored or processed;

(c) material changes to controls;

(d) material changes to underlying infrastructure, including networking, hosting or operating environment;

(e) material changes to the technology stack used for the Service; or

(f) changes in the geographical jurisdictions from which the Services are delivered or in which the Purchasing Agency Data are stored or processed;

Good Industry Practice means, in relation to your performance of the Services, the exercise of the skill, diligence, prudence, foresight and judgement that would be expected from a highly skilled and experienced person engaged in the same type of undertaking under the same or similar circumstances;

Tier 1 Security Assurance and Risk Rating means the highest level of security assurance that a provider can obtain for a Services Listing in the Marketplace;

Tier 1 Services means the Services for which you have sought and obtained a Tier 1 Security Assurance and Risk Rating, for as long as that rating remains in place; and

Trigger Event has the meaning in clause 7.2(b).