

December 31, 2022

John Smith
Chief Executive Officer
Pillar**Service Auditor's Engagement Letter for AssuranceLab's Establish Package: Type 2 Assurance Reports****Objective and Scope of the engagement**

You have requested that we undertake a reasonable assurance engagement on Pillar's Statement, regarding the design of controls over Pillar's Software as a Service System system, the description of Pillar's Software as a Service System system, and the operating effectiveness of the controls for the Type 2 report(s). You will provide this description, which will accompany our report. The Type 2 audit period will commence upon a date nominated by Pillar and will cover an audit period between 6-12 months total. The description of Pillar's Software as a Service System system comprises control objectives and related controls designed to achieve those objectives for that period.

The standards, control objectives and criteria to be addressed, as well as the reporting standards to be used to issue the reports include the Trust Services Criteria are issued by the AICPA. You have selected the Trust Services Criteria for the Common Criteria/Security, Availability and Confidentiality. The report(s) will be issued using the AT-C 105 and 205 standards.

We are pleased to confirm our acceptance and our understanding of this reasonable assurance engagement by means of this letter. Our assurance engagement will be conducted with the objective of expressing an opinion on Pillar's Statement regarding the suitability of the design of controls within Pillar's Software as a Service System system to achieve the stated control objectives, the fair presentation of the description of Pillar's Software as a Service System system, and the operating effectiveness of those controls throughout the period.

Responsibilities of the assurance practitioner

We will conduct our assurance engagement in accordance with, AT-C 105 and 205 assurance engagements for, SOC 2 respectively. These standards require that we comply with ethical requirements applicable to assurance engagements and plan and perform procedures to obtain reasonable assurance about whether, in all material respects, Pillar's Statement that the controls are suitably designed to achieve the control objectives, the description of Pillar's Software as a Service System system is fairly presented, and the controls operated effectively throughout the period is fairly stated. An assurance engagement involves performing procedures to obtain evidence about the design, description, and operating effectiveness of controls. The procedures selected depend on the assurance practitioner's professional judgement, including the assessment of the risks of material deficiencies in the design of controls, misstatements in the

description or deviations in the operating effectiveness of controls within Pillar's Software as a Service System system.

Because of the inherent limitations of an assurance engagement, together with the inherent limitations of any system of controls there is an unavoidable risk that some deficiencies in the design, misstatements in the description or deviations in the operating effectiveness of controls may not be detected, even though the engagement is properly planned and performed in accordance with Standards on Assurance Engagements.

The system, within which the controls that we will test operate, will not be examined except to the extent the system is relevant to the achievement of the control objectives. Accordingly, no opinion will be expressed as to the effectiveness of the system of controls as a whole.

Responsibilities of Pillar

Our assurance engagement will be conducted on the basis that Pillar management acknowledges and understands that they have responsibility:

1. for the preparation of a written Statement that throughout the period, in all material respects, and based on suitable criteria:
 - 1.1. the controls within Pillar's Software as a Service System system were suitably designed to achieve the identified control objectives; and
 - 1.2. the description fairly presents Pillar's Software as a Service System system as designed, including changes in controls; and
 - 1.3. the controls stated in Pillar's description of its system operated effectively to achieve the control objectives;
2. for the identification of the suitable standards, control objectives and criteria to meet end user requirements;
3. for the identification of risks that threaten achievement of the standards, control objectives and criteria identified;
4. for design of the system, comprising controls which will mitigate those risks so that those risks will not prevent achievement of the identified control objectives and therefore that the control objectives will be achieved;
5. for preparation of a description of the system, including identification of any controls operated by a third party, service or sub-service organisation and whether the inclusive or carve-out method has been used in relation to those third party controls;
6. for operation of the controls as designed throughout the period;
7. to provide us with:
 - 7.1. access to all information of which those charged with governance and management are aware that is relevant to the description of Pillar's Software as a Service System system and design of the controls within that system;
 - 7.2. additional information that we may request from those charged with governance and management for the purposes of this assurance engagement; and
 - 7.3. unrestricted access to persons within the entity from whom we determine it necessary to obtain evidence.

As part of our assurance process, we will request from management and, where appropriate, those charged with governance, written confirmation concerning representations made to us in connection with the engagement.

Assurance Approach and Procedures

We will examine and evaluate the control objectives, criteria and controls for the Software as a Service System system described above.

Our procedures will extend to the control objectives, criteria and related controls at relevant third parties only to the extent that those controls are included in Pillar's description of the Software as a Service System system and are necessary to achieve the relevant control objectives.

Due to the complex nature of internal control, our assurance procedures will not encompass all individual controls at Pillar, but will be restricted to an examination of those controls reported which achieve the control objectives identified by the responsible party in the "Description of the Software as a Service System" provided to us.

Our assurance procedures are likely to include:

1. obtaining an understanding of the control environment of Pillar relevant to the Software as a Service System system;
2. evaluating the design of specific controls by:
 - 2.1 assessing the risks that threaten achievement of the control objectives; and
 - 2.2 evaluating whether the controls described are capable of addressing those risks and achieving the related control objectives;
3. evaluating the completeness, accuracy and presentation of the Description of the Software as a Service System System against the controls as designed; and
4. making enquiries, inspecting documents, conducting walk throughs and re-performance of controls to ascertain whether the degree of compliance with controls is sufficient to achieve their control objectives throughout the period (Type 2).

Assurance Report

The format of the report will be in accordance with, AT-C 105 and 205 with respect to reasonable assurance engagements and will consist of an opinion on the description and an accompanying description of the tests of controls that we performed and the results of those tests. Our opinion will be phrased in terms of Pillar's Statement regarding the suitability of the design of controls to achieve the control objectives, the fair presentation of the description and the operating effectiveness of controls as designed.

Our reports are prepared for the use of Pillar for the purpose of sharing with your customers and regulators and should not be used for any other purpose. The assurance report will be prepared for this purpose only and we disclaim any assumption of responsibility for any reliance

on our report to any person other than Pillar and its customers, regulators, or for any purpose other than that for which it was prepared.

Material Deficiencies in Design, Misstatements in Description or Deviations in Operating Effectiveness of Controls

We will issue an assurance report without modification, to provide a reasonable assurance conclusion on the controls within the Software as a Service System system where our procedures do not identify a material deficiency in the design of controls necessary to achieve the control objectives, misstatement in the description of the Software as a Service System system by the responsible party, or deviation in the operating effectiveness of controls as designed. For this purpose, a material deviation, misstatement, or deficiency exists when:

- (a) the controls as designed or the degree of compliance with them will not or may not achieve the control objectives in all material respects or the description contains material inaccuracies, inadequacies or omissions; and
- (b) knowledge of that deficiency, misstatement, or deviation would be material to users of the assurance report.

For Type 2 reports, if our assurance engagement discloses that there are material deficiencies in the design or deviations in the operating effectiveness of controls during the period covered by the report, such deficiencies will be disclosed in our report even if they were corrected prior to the end of the reporting period. However, our report will indicate that such deviations were corrected if that is the case. If any material deficiencies disclosed in our report have been corrected subsequent to this period (or are in the process of being corrected), we will refer to this in our report.

Engagement Timing

AssuranceLab conducts an agile audit process that completes the audits at the pace set by Pillar's team. Following the execution of this Agreement, the project will be created with all of the document requests required to complete the Type 2 audits. Documents can be uploaded by Pillar at any time. AssuranceLab's team maintains service level standards of responding to client queries within 24 hours and reviewing uploaded documents within 3 business days. The timeline to completion of the engagements is dependent on Pillar providing the necessary documentation and responding to queries raised by AssuranceLab until the audits are complete.

Engagement Fees

<<Redacted>>

Confirmation of agreement

Please confirm your acceptance of the agreement by signing the enclosed copy and returning it to us.

Yours faithfully,

Erika Villanueva

Erika Villanueva CA

AssuranceLab

Copy letter to be returned to AssuranceLab

I accept the terms of the agreement for and on behalf of Pillar.

.....
Signed John Smith, Chief Executive Officer

.....
Date

Terms of business

1. Services

- 1.1. We will perform the services described in this engagement letter with reasonable skill and care. You confirm that the scope is sufficient for your purpose. The services (including deliverables) are provided solely for you for the purpose set out in the engagement letter or the relevant deliverable.
- 1.2. You may not disclose a deliverable or make the benefit of the services available to anyone else or refer to the contents of a deliverable or the findings of our work, except (i) as stated in the engagement letter, (ii) with our prior written consent on terms to be agreed, (iii) where required by law or regulation, or (iv) to your lawyers or group members as long as you tell them, in advance, that we accept no liability to them and that no onward disclosure may be made.
- 1.3. We accept no liability to anyone, other than you, in connection with our services, unless otherwise agreed by us in writing.
- 1.4. Either we or you may request a change to the services or this agreement. A change will be effective only when agreed in writing.
- 1.5. You may rely only on our final written deliverables and not on oral advice or draft deliverables. If you wish to rely on something we have said to you, please let us know so that we may prepare a written deliverable on which you can rely.
- 1.6. In performing the services, we will not be deemed to have information from other services.

2. Materials

- 2.1. For compliance purposes, we are required to retain the final audit file for 7 years. This includes any evidence and documentation provided by Pillarto support our audit conclusions. All materials and the final audit file are subject to confidentiality including clause 8.1 below.
- 2.2. We will endeavour to limit our requests to only those materials required to deliver the services and to support redacted documents to protect confidentiality.

3. Liability

- 3.1. You agree that we will not be liable for (i) loss or corruption of data from your systems, (ii) loss of profit, goodwill, business opportunity, anticipated savings or benefits or (iii) indirect or consequential loss.
- 3.2. You agree that our total liability (including interest) for all claims connected with the services or this agreement (including but not limited to negligence) is limited to 10 times the fees payable for the services (excluding GST) or \$250,000, whichever is the greater.
- 3.3. Nothing in this agreement will limit a person's liability for (i) death or personal injury caused by that person's negligence, (ii) that person's fraud or (iii) anything else that cannot by law be limited.

4. Distributions

- 4.1. The audits conducted and reports prepared are intended for users of Pillar's Software as a Service System. Pillaris wholly responsible for the distribution of these reports and should only do so in their complete form with appropriate disclaimers when shared with any other parties. AssuranceLab assumes no responsibility for the reports being shared in partial form or with any other parties that were not users of Pillar's Software as a Service System at the time of the audits being completed. AssuranceLab will not disclose the reports to any party unless required to do so by law or for compliance purposes.

5. Your responsibilities

- 5.1. In order for us to guide you properly and complete the services you will make sure that (i) any information given to us by you, or anyone else working with or for you, is (a) given promptly, (b) accurate and (c) complete; and (ii) any assumptions are appropriate.
- 5.2. We will not verify all information given to us relating to the services. Our performance depends on you performing your obligations under this agreement.
- 5.3. We are not liable for any loss arising from you not fulfilling your obligations.

6. Fees

- 6.1. You agree to pay us for our services.
- 6.2. Our fees may reflect not only time spent, but also such factors as complexity, urgency, inherent risks, use of techniques, know-how and research together with the level of skills and expertise required of the personnel needed to perform and review the services.
- 6.3. You will also pay any taxes, including GST, that are due in relation to our goods and services.
- 6.4. All invoices are payable within 30 days of the date on the invoice.

7. Confidentiality

- 7.1. We and you agree to use the other's confidential information only in relation to the services, and not to disclose it, except where required by law or regulation or where required by a professional body of which we are a member.
- 7.2. We may wish to refer to you and the services we have performed for you when marketing our services. You agree that we may do so, as long as we do not disclose your confidential information.
- 7.3. You agree that we may perform services for your competitors or other parties whose interests may conflict with yours, as long as we do not disclose your confidential information and we comply with our ethical obligations.

8. Data protection

- 8.1. We may process personal data received from you, or anyone else working with or for you, for the purposes of any of (i) providing the services, (ii) maintaining and using relevant IT systems, (iii) quality and risk management reviews, (iv) providing you with information about us and our range of services, and (v) complying with any requirement of law, regulation or a professional body of which we are a member.
- 8.2. You confirm that you have all necessary authority from all relevant data subjects for us to use and disclose such personal data in accordance with the agreement.
- 8.3. Where we act as your data processor, we will act only on your lawful instructions and we will comply with obligations equivalent to those imposed on you to take appropriate security measures against access to, or alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing in accordance with our obligations.

9. Termination

- 9.1. Either we or you may end this agreement immediately by giving written notice to the other if (i) the other materially breaches it and does not remedy the breach within 14 days, (ii) the other is or appears likely to be unable to pay its debts or becomes insolvent or (iii) the performance

of it (including the application of any fee arrangements) may breach a legal or regulatory requirement.

- 9.2. Either we or you may end this agreement on 30 days' written notice subject to the minimum 12 months of fees where any final reports are issued in accordance with this agreement.
- 9.3. You agree to pay us for all services we perform up to the date of termination.
- 9.4. If the termination is based on substandard services or any disagreement that cannot be mutually resolved, we will return the service fees and endeavour to assist you in transitioning to a new service provider without any transition costs.

10. Dispute resolution

- 10.1. If a dispute arises, the parties will attempt to resolve it by discussion, negotiation and mediation before commencing legal proceedings.
- 10.2. This agreement and any dispute arising from it, whether contractual or non- contractual, will be governed by Australian law and be subject to the exclusive jurisdiction of the Australian courts.
- 10.3. Any claims must be brought no later than 2 years after the date the claimant should have been aware of the potential claim and, in any event, no later than 4 years after any alleged breach.

11. General

- 11.1. We may be obliged in certain circumstances by law or by professional requirements to make disclosures to statutory or regulatory authorities.
- 11.2. No party will be liable to another if it fails to meet its obligations due to matters beyond its reasonable control.
- 11.3. This agreement forms the entire agreement between the parties in relation to the services. It replaces any earlier agreements, representations or discussions.
- 11.4. Where you consist of more than one party, an act or omission of one party will be regarded as an act or omission of all.
- 11.5. Any clause that is meant to continue to apply after termination of this agreement will do so, including but not limited to confidentiality and data protection.