Safer Technologies for Schools Assessment:

Supplier Guide

(previously known as the ST4S Vendor Guide)

Guide for suppliers participating in the Safer Technologies for Schools Assessment process (ST4S) covering Australian and New Zealand controls

Release:	2022.1
Date of this version:	21-Oct-22
Author:	ST4S Team
Document Version Number:	1.02 Final
Location:	Latest official version available www.st4s.edu.au

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Important information including disclaimer:

This guide is provided:

- for information purposes only and does not constitute advice;
- on the basis that suppliers are responsible for assessing the relevance and accuracy of its content.

Education Services Australia Limited through its business unit the National Schools Interoperability Program (NSIP) has compiled this guide in good faith and has endeavoured to ensure that all material is accurate and does not breach any entity's rights at the time of its inclusion. However, the material may contain unintentional errors and is provided 'as is'.

Participation in the Safer Technologies for Schools (ST4S) process is voluntary. An entity which chooses to participate in the ST4S process acknowledges and agrees that:

- the ST4S process and results depend entirely on the answers provided by an entity and the point of time at which such answers are provided;
- the ST4S assessment of an entity may result in a recommendation to participating education authorities that such entity's product not be used until security/privacy issues are remedied; and
- NSIP is conducting the ST4S assessments on behalf of participating jurisdictions for the purpose of ensuring consistency in security/privacy assessments and to protect data including the personal information of students.

To the extent lawful, NSIP:

- excludes all warranties in respect of the guide and the ST4S assessment process;
- is not liable for any loss or damage (direct or indirect) resulting from the use of the guide or participation in or the results of, the ST4S assessment process; and
- will not be liable for any incidental, special or consequential damages of any nature arising from the use of or inability to use the guide or participation in the ST4S assessment process.

Links provided to other websites are provided for the user's convenience and do not constitute endorsement of those sites. ESA is not responsible for material contained in any website that is linked to from this guide.

If you use the links provided in this guide to access a third party's website, you acknowledge and agree that the terms of use, including licence terms, set out on the third party's website apply to the use which may be made of the materials on that third party's website. If this guide contains links to your website and you have any objection to such link, or if you have any questions regarding use of material available on or through this website, please contact us (assessment@st4s.edu.au).

Unless otherwise indicated, the copyright in this Supplier Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Supplier Guide without the prior written permission of Education Service Australia Ltd.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Contents

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Version Control & Latest Version

Note: The latest copy of the ST4S Supplier Guide is available from www.st4s.edu.au

Version Control			
Version	Date:	Author/Organization:	Comments
V0.1	26/07/2022	ST4S Team	Draft release of 2022 framework
V0.2	27/07/2022	ST4S Team	Updates to PF29, PF30, PF31. Change vendor to supplier.
V0.3	01/08/2022	ST4S Team	Updates to P2D and P2E
V0.4	15/08/2022	ST4S Team	Incorporated feedback from ST4S Working Group
V0.5	29/08/2022	ST4S Team	Changes to PR10 and S1, S3
V1.0	31/08/2022	ST4S Team	Document made final
V1.01	5/9/2022	ST4S Team	Added AU and NZ ISM versions reference. Corrected missing element from question S1 & S3 response option D (ECDH). Update to NZISM reference in control A6.
V1.02	5/10/2022	ST4S Team	Added integrator controls PF40-PF50. Retired control PF34. Updated PR11 question wording and answer options re: Opt-in/out commercial mailing lists. Updated PF38 question text.

1. Introduction

1.1 Purpose

This supplier guide provides guidance and information regarding:

- the assessment process;
- the initial categorisation of services/products based on assessment tiers (see Appendix A);
- the questions that make up the questionnaire;
- the minimum and indicative responses to the questions and links to relevant industry standards;
- the clarification process; and
- the assessment results and how they will be shared with participating member organisations.

1.2 Terminology

Table 1.1: Terminology

Term	Definition
Education authority	Government or non-government ST4S member organisations responsible for ICT guidance to schools and other compulsory sector education providers in a given jurisdiction
Jurisdiction	Country, State or Territory participating in ST4S
ESA	Education Services Australia Limited (www.esa.edu.au)
NERA	National Education Risk Assessment (name changed to ST4S Assessment)
ST4S	Safer Technologies for Schools (www.st4s.edu.au)
ST4S WG	Safer Technologies for Schools Working Group
ST4S VG	Safer Technologies for Schools Supplier Reference Group
NSIP	National Schools Interoperability Program (www.nsip.edu.au), a business unit of ESA

1.3 Background

- Schools, kura (in New Zealand) and school system authorities have obligations stemming from Federal/National and State legislation to protect the privacy and security of official information and personal information held on behalf of students, parents and staff. As the role of ICT in schools has expanded and the range of online products and services has increased, the need for a rigorous and systematic approach to managing information risk and facilitating system integration has also increased.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

- The need for information risk mitigation also aligns with efforts to improve online safety for students. In 2018 the Council of Australian Governments (COAG) endorsed the National Principles for Child Safe Organisations, based on the Royal Commission's Child Safe Standards. In New Zealand, the Child and Youth Wellbeing Strategy (2019) seeks to improve the safety and wellbeing of all children, including in the online context (https://www.childyouthwellbeing.govt.nz/)
- As schools adopt new digital products and services, the need to streamline the on-boarding and integration of applications increases. Integration using agreed standards and APIs rather than bespoke manual data exchange (no effective integration) is key to learner centric data management and minimising administrative overheads as well as optimising privacy and security.
- At the request of the National Schools Interoperability Program Steering Group, the NSIP Team worked with agency and sector representatives to develop a standardised set of online education services risk and interoperability assessment criteria. Subject matter experts from agencies and the non-government school sectors meeting as the ST4S Working Group have developed a common evaluation process and assessment criteria covering the key domains of trust namely: security, privacy, interoperability and online safety.
- As suppliers develop and market new digital products and services to schools, they need to be aware of user safety considerations and the role that their services play in shaping online environments. The Australian eSafety Commissioner's Safety by Design is designed to provide online and digital interactive services with a universal and consistent set of realistic, actionable and achievable measures to better protect and safeguard citizens online. Suppliers are encouraged to become familiar with the SbD principles. Tools and resources to support suppliers to embed user safety into the design of their products or services will be made available on the eSafety website throughout 2020.
- Safer Technologies for Schools (ST4S) commenced in 2020 in Australia following a pilot (known as the National Education Risk Assessment in 2019).
- The New Zealand Ministry of Education | Te Tāhuhu o Te Mātauranga Aotearoa, joined ST4S in 2021.

1.4 Benefits of a coordinated approach

- Most schools and school system authorities have established local risk assessment teams or are planning to do so.
- The anticipated benefits of a coordinated assessment approach are as follows:
    - Agreed standards and practices for the management, exchange and use of personal information in schools are clearly communicated to all school communities and product suppliers.
    - School selection of online services is guided by reliable information about privacy, security and interoperability.
    - Reduced cost, effort and time for education authorities in assessing and on-boarding online services for schools.
    - Increased transparency and trust regarding the data exchanged with service providers.
    - Reduced cost and time for suppliers to demonstrate compliance with national security, privacy and interoperability standards.
    - An incentive for suppliers to comply with security, privacy and interoperability standards.

1.5 High Level Assessment Process & Prioritisation

The ST4S Assessment process consists of 3 steps:

1. Suppliers complete a self-directed ST4S Readiness Check (refer www.st4s.edu.au/readiness-check) to determine eligibility.
2. Eligible services are prioritised by the ST4S Working Group.
3. Prioritised services undergo a full ST4S assessment in collaboration with the ST4S Assessment team.

Importantly, the ST4S Working Group, in consultation with the NSIP Steering Group, is responsible for determining the assessment priority of supplier products and services. Each assessment period a limited number of services can

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

undergo a full ST4S assessment. Results from the Readiness Check do not guarantee a priority invitation to complete, or compliance under, the full ST4S assessment.

2. Assessment process

A typical ST4S assessment consists of 3 steps:

1. The software supplier, at the request of schools or through their own initiative, completes an ST4S Readiness Check. If the Readiness Check outcome indicates that the product or service is 'eligible' for a full assessment, the supplier can optionally submit their product or service for prioritisation.
2. Products and services submitted for full assessment are prioritised by the ST4S Working Group. This group meets monthly and is made up of security and privacy professionals from the education sector across Australia and New Zealand. Products and services are prioritised based on members' needs and consultation with their schools.
3. Once prioritised, suppliers are invited to participate in a 'full' ST4S assessment of their product or service.

Please refer below for more details.

2.1 Readiness Check

The Safer Technologies 4 Schools (ST4S) Readiness Check is a self-assessment tool for suppliers. It allows suppliers to check how their product compares against the agreed privacy and security assessment framework for primary and secondary education (the ST4S assessment framework).

The ST4S Readiness Check is suitable for products and services that are used within a primary/secondary education setting and which process or handle personal or sensitive information and operate in an online environment (whether partially or entirely).

The ST4S Readiness Check consists of two steps:

- A short survey that presents critically important criteria. Upon completing the survey suppliers will be provided with some feedback about their service's readiness to complete a full ST4S assessment.
- An optional step to submit the service to be considered for a full ST4S assessment.

Once suppliers have completed the Readiness Check, the readiness status of the service will be displayed.

If the service is not ready to submit for full assessment, suppliers can return later to update responses once the recommended changes have been incorporated.

If the service is ready, suppliers can submit their results to the ST4S Working Group for consideration and prioritisation for a full ST4S assessment.

Questions in the Readiness Check:
The following questions (as identified by reference numbers in this guide) are presented to suppliers in the Readiness Check:

Framework section	Control questions in Readiness Check
Company and product details	C1, C4, C5
Product information	P1, P2, P3, P4, P5, P6, P9, P10, P11, P12, P13
Hosting and location	H1, H5

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Security – Technical	S1, S3, S4, S5, S7, S8, S9, S10, S11, S13
Access	A1, A2, A5, A6, A7, A10, A11, A13, A16A, A16B
HR	HR1, HR2, HR3
Processes and testing	T1, T2, T3, T6, T7
Plans and quality	Q5
Data deletion and retention	D3, D4,
Compliance controls	CC2
Privacy – Requests	PR1, PR1A, PR2, PR10, PR12, PR13, PR14
Privacy - Functionality	PF4, PF6*, PF7*, PF8*, PF9*, PF10*, PF13*, PF14*, PF18*, PF36

Please note that functionality questions marked with * are presented based on the response to PF4.

Learn more about the ST4S Readiness Check here: www.st4s.edu.au/readiness-check

2.2 Full Assessment Process

Suppliers that complete the Readiness Check and are prioritised for full assessment will be invited by the ST4S Assessment Team to proceed and undertake a full assessment. This may occur days, weeks or months following the original Readiness Check submission.

Suppliers will be provided a link to the detailed ST4S questionnaire and asked the full set of ST4S control queries as represented in this guide.

2.2.1 Generation of School Level Reports

The responses and any supporting evidence provided by suppliers to the questionnaire will be assessed against the ST4S assessment criteria and, if necessary, reviewed internally by the ST4S Assessment Team and / or the ST4S WG. The ST4S assessment criteria and responses are updated from time to time as approved by the ST4S WG. Where suppliers have missed a question or not provided sufficient detail, the assessment team may follow up with the submitting supplier to ensure a fair and accurate response is gathered and assessed. Where a response cannot be obtained from a supplier, the most conservative response will be recorded in order to facilitate the completion of the questionnaire.

2.2.2 Release of findings to suppliers

Suppliers will receive a draft of the school level report which is generated based on the responses provided to the supplier questionnaire. Suppliers may also receive a spreadsheet containing questions on which the assessment team is seeking further clarification. Suppliers are asked to respond to the clarifications within the timelines as directed. Supplier responses to the clarifications and a commitment to rectify any risks resulting in a 'non-compliant' outcome may alter the school report.

Following the conclusion of clarifications, suppliers should expect to receive a final school level report in approximately four weeks. A copy of the final school level report will be provided to the supplier's nominated contact. The exception to this release timeline is where a supplier has received a non-compliant outcome. Suppliers will be notified if this is the case and informed of applicable timeframes.

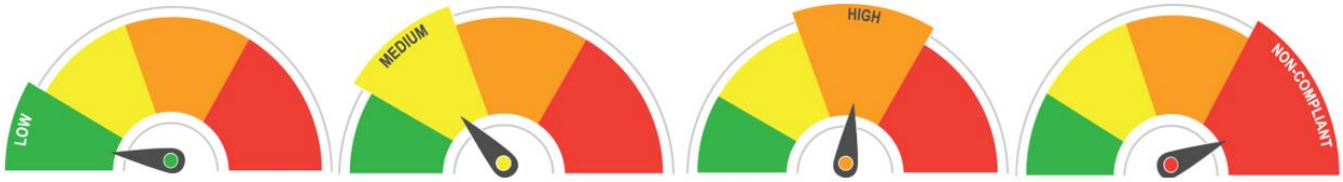
Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

2.2.3 Findings outcomes

The possible assessment outcomes depend on the 'tier' of the product or service. Tiering is dependent largely on the data processed or stored and functionality offered. To learn more about tiers, refer to Appendix A.

For Tier 1 and 2 services, the assessment of a product or service results in one of the following outcomes:

Low risk *Medium risk* *High risk* *Non-compliant*



The overall assessment outcome is the highest risk level remaining after all available treatments have been applied. A 'Non-compliant' assessment outcome is assigned when a mandatory minimum standard is not met. The assessment outcome appears on the front page of the school level report.

For Tier 3 services, the assessment of a supplier's product or service results in one of the following outcomes:

Use Responsibly *Use with Caution*

2.2.4 What do findings outcomes mean?

In typical school settings, there is always some risk in using a product/service. Some products/services may receive a Medium or High rating simply because of the types of functionality that they offer (for example remote access, the use of webcams, ability to chat with members of the public). The overall assessment outcome highlights to schools that in using the product/service there are treatments that need to be applied (e.g., configuration, reviewing of logs). Assigning a Medium, High, or Use with Caution outcome to a product/service is intended to draw school users' attention to the fact that treatments need to be reviewed and implemented when using the particular product/service. Typically, besides removing the particular functionality in question, there is little or nothing a supplier can do to reduce the overall assessment outcome to Low.

Products/services which have fundamental compliance gaps will be tagged as being 'Non-Compliant'. Each education authority will determine what suggestion they provide to schools when using products/services which receive this assessment outcome.

2.2.5 Challenging findings

As part of the development of the final school level reports, suppliers will have been provided a draft copy of the school level report and clarification questions. The final school level report should not be a surprise to the supplier as the outcomes are dictated by the guidance in the ST4S Supplier Guide. If a supplier considers a school level report is not accurate, that supplier may lodge a request to have their report re-reviewed. In order to request a re-review, suppliers need to provide relevant details to the contact point detailed in Section 4 below.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

2.2.6 Re-assessment

Subject to resourcing and prioritisation, suppliers may be invited to be re-assessed based on a number of factors, including time since original assessment, updates to the ST4S standards, updates to the supplier product/service and/or occurrence of a breach or security incident.

2.2.7 Changing the school level report

The final school level report can only be altered by the ST4S Team where there are factual errors. Please contact the ST4S Team if you consider this to be the case.

3 Sharing and use of full assessment reports

3.1 Findings distribution

The ST4S Team provides assessment findings (including raw results and school level reports) to the NSIP Steering Group (typically Education CIOs) and the ST4S WG (Chief Information Officer nominated security and privacy representatives). The ST4S Team do not distribute findings to schools directly. The process and timelines by which each education authority distributes findings is a local matter. In some education authorities, findings will be distributed to schools within days of release from ST4S, in others, schools need to make requests directly to their local education authority.

3.2 Sharing of findings with Trusted Parties

When responding to the questionnaire suppliers should be aware that results will be shared with the NSIP Steering Group (http://www.nsip.edu.au/about-nsip) and other parties as nominated by the NSIP Steering Group (including the NZ Ministry of Education). This may include central department or sectoral staff and their schools and /or regional offices.

In addition, subject to approval by the NSIP Steering Group and the ST4S WG, results may be distributed to other parties without prior notice or consultation with the relevant supplier.

3.3 Sharing of findings with Suppliers

Suppliers will be provided with a copy of their school level report. These guidelines are intended to provide a sufficient level of detail so that suppliers can effectively perform a self-assessment against the assessment criteria. However, where there are critical risks the ST4S assessment team may contact suppliers directly to communicate any issues identified.

The ST4S assessment team will not provide suppliers with the findings of other suppliers who have submitted responses.

3.4 Supplier use of the findings internally

One of the goals of the ST4S process is to influence suppliers to improve, privacy, security, online safety and interoperability approaches in the design, build, testing, deployment, maintenance, configuration and end-user training regarding their product/service. Suppliers can continue to improve their products/services over time and are encouraged to continue to reference the ST4S standards (as documented in the ST4S Supplier Guide) as it is updated over time.

3.5 Guidance regarding Supplier use of assessment outcomes

Suppliers receive copies of the final assessment reports with the following caveats and conditions:

1. ST4S reports will be marked as “Not for commercial purposes”
2. Suppliers must not provide the ST4S assessment report or any copies or extracts of it to anyone outside the supplier organisation (for example, schools or school communities).

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

3. Suppliers may notify existing and prospective customers that they have participated in the ST4S process and meet the minimum required ST4S standards (against a specific version of the ST4S assessment standards) for the specific version of their product/service.
4. Suppliers must acknowledge and communicate with customers that an ST4S assessment outcome does not necessarily mean that the supplier is compliant with local State/Territory/Country or Non-Government sector requirements.
5. Suppliers must direct enquiries from schools regarding the provision of detailed reports to the relevant education authority (Government schools to the relevant State/Territory Department or Ministry of Education, Australian Catholic schools to their local State or Diocese office and Australian Independent schools to their State/Territory association) as listed on the final report.
6. Suppliers must not edit or modify their final or draft school-level reports in any way.
7. Suppliers must not claim that a ST4S assessment applies to other products, services, or modules offered by the supplier, or different versions of the product, service or module.
8. Suppliers must not publish, advertise or promote their specific assessment outcome (low/medium/high), or use or extract any part or portion of their ST4S report. Communications to existing and prospective customers must be limited to the particular service version that has been assessed and the result, and must indicate that this version aligns to a particular ST4S assessment standard version (compliance assessments are not enduring for all time).
9. Suppliers must not claim or imply that ST4S is an endorsement, recommendation, or approval of the product/service or a guarantee that the service is fit for purpose.
10. Suppliers must not publish in whole or in part the ST4S assessment results for another supplier's service.
11. Suppliers must notify the ST4S Assessment Team if they come into possession of some or all of another supplier's ST4S report or results.
12. If a supplier does not comply with the above usage conditions, the ST4S Assessment Team may rescind/withdraw/modify that supplier's assessment outcome.
13. In its sole discretion, the ST4S Assessment Team may rescind/withdraw/modify any assessment outcome at any time.

These guidelines will be updated from time to time. Please refer to the ST4S website (www.st4s.edu.au) for the latest usage conditions.

Suppliers should direct Australian government school queries to the relevant educational jurisdiction listed below:

- Government Schools:
  - NSW information.security@det.nsw.edu.au
  - QLD riskreviews@qed.qld.gov.au
  - SA education.ictcybersecurity@sa.gov.au
  - TAS security@education.tas.gov.au
  - NT cloudsystems.doe@ntschools.net
  - WA privacy@education.wa.edu.au
  - VIC infosafe@education.vic.gov.au
  - ACT DSST@act.gov.au

Suppliers should direct Australian non-government school queries to the relevant authority listed below:

- Catholic and Independent Schools
  - Catholic Education – Contact the relevant local jurisdiction ie diocese, CEnet or commission.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

- Independent schools – Contact the local AIS operating in your State or Territory.

Suppliers should direct New Zealand school enquiries to: cyber.security@education.govt.nz

Requirements for Non-compliant and Non-participating suppliers:

1. If approached by current or potential customers regarding the ST4S process, suppliers should note that their outcome was non-compliant or non-participating and direct schools to the relevant educational jurisdiction, Catholic Education officer or the Association of Independent Schools, as listed above.

Disclaimer in relation to Supplier Guide:

1. This Supplier Guide is provided for your information only and you are responsible for ensuring that its contents are current, complete and accurate before using it.
2. Whilst ESA has endeavoured to ensure that the Supplier Guide is accurate and up-to-date, the Supplier Guide is provided to you on an 'as is' basis and you use it at your own risk.
3. To the extent lawful, NSIP:
    - excludes all warranties in respect of the Supplier Guide; and
    - is not liable for any loss or damage however caused resulting from the use or inability to use the Supplier Guide or caused to any property as a result of the use of the Supplier Guide.

4 Support

Queries relating to ST4S can be raised via email here assessment@st4s.edu.au

5 Instructions for responding to questionnaire

5.1 Important information and disclaimer in relation to the questionnaire.

If you do not agree to any of the points below, you must not complete a ST4S assessment questionnaire.

- **Responses provided may be used to inform any contractual arrangements entered into by government departments, non-government sectoral authorities or individual schools.**

- **Please note that the ST4S school-level reports resulting from participation in ST4S do not constitute an endorsement, approval or recommendation regarding the use of the product/service to which they apply, nor do they constitute advice regarding the quality or licensing of, or the decision to purchase or use a particular product or service. ST4S assessment outcomes are provided with no guarantee or warranty.**

- For the purpose of a ST4S assessment questionnaire, a reference to "Solution" means the ICT system/s your organisation intends to use to capture, store and process personal, departmental, sectoral or education data (or any form of official data).
- You may be required to provide evidence at a later date to support your responses.
- This questionnaire is:
    - necessary to meet due diligence requirements of education data being stored and used outside of internal networks or in products/services that have the ability to communicate with external networks/systems; and
    - specifically designed to elicit detail of the product, service or solution in order to inform potential end-users of the product, to detail any potential risks and mitigations and to arrive at an overall risk rating.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

- Participating stakeholders outside of the ST4S assessment team may seek further detail from suppliers to address local cyber security and information security needs at a future date.
- Engagement in the assessment process and /or completion of the questionnaire does not guarantee or indicate any intention to proceed with purchasing, licensing or procurement activities.
- Participation in any stage of the ST4S assessment process or otherwise in relation to any matter concerning the ST4S assessment process, will be at each supplier's sole risk, cost and expense. NSIP will not be responsible for any costs or expenses incurred by a supplier in preparing its response to the questionnaire or otherwise taking part in the ST4S assessment process or taking any action related to the ST4S assessment process.
- The ST4S assessment process is not an offer capable of acceptance by any person or entity or as creating any form of contractual, quasi contractual or any other rights based on legal or equitable grounds. Therefore, engagement in the ST4S assessment process and /or completion of the questionnaire does not constitute an agreement, arrangement or understanding between a supplier and NSIP, the assessment service or any stakeholders in ST4S.
- NSIP is not liable to any supplier or any other entity on the basis of any legal or equitable grounds including negligence or otherwise as a consequence of any matter or thing relating or incidental to a supplier's participation in the ST4S assessment process.
- The questions below directly relate to the requirements contained within the various and relevant privacy acts and the various Government information security classification frameworks. Supplier responses will assist in the assessment, mitigation and monitoring of the risks associated with their product/service.

5.2 Completion of the Questionnaire

- Suppliers will receive, via email, a link to complete a questionnaire for a specific nominated service/product. A survey access pin will be sent via text message to the nominated contact.
- Suppliers ideally make a submission for both Australian and New Zealand education authorities. Where suppliers only operate in one country they may elect to submit for a single country.
- All questions are mandatory, and suppliers will not be able to navigate between pages without first completing the questions on the page displayed.
- If at any time suppliers are not sure which product, module or component is the subject of the response, please contact the assessment team.
- If the supplier's service offers a 'for school use' and a 'for home use' version, please complete the questionnaire based on the 'for school use' version.
- If suppliers need to provide any attachments which are directly relevant to the question being asked (please do not provide advertising materials or lengthy documents) prefix the file name with the relevant question ID e.g. INT3-API Product XYZ).
- Suppliers will be able to partially complete the questionnaire and return at a later time to complete it.
- Suppliers may choose to download a copy of their responses to the questionnaire prior to submitting.
- Suppliers can contact the assessment team (assessment@st4s.edu.au) if they have any questions or comments. We are here to help.

5.3 Accuracy of Responses to the Questionnaire

In submitting the questionnaire, suppliers must:

- confirm all information provided in response to the questionnaire is true, correct, accurate, up-to-date, and not misleading in any way;
- acknowledge that:
    - the ST4S assessment team will rely on the information provided in response to the questionnaire to assess the service's compliance and provide guidance to stakeholders;

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

- incomplete, inaccurate, out of date or misleading information may result in the relevant service receiving an inaccurate or misleading report; and
- agree to provide further information or evidence to support the questionnaire responses if requested.

5.4 Timeline

Timelines to submit the self-assessment questionnaire are included in the assessment information email sent to suppliers.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

6 Assessment Criteria

6.1 Criteria – Company & product detail

#	Question	Tier	Notes
C0	For which countries are you submitting an ST4S survey response?	1 & 2	Response options: A. Australia and New Zealand B. Australia only C. New Zealand only
C1	Vendor name	1 & 2	Informational
C2A	Vendor ABN	1 & 2	Informational (AU submissions)
C2B	Vendor NZBN	1 & 2	Informational (NZ submissions)
C3A	Registered Australian address of vendor	1 & 2	Informational (AU submissions)
C3B	Registered New Zealand address of vendor	1 & 2	Informational (NZ submissions)
C4A	Country in which the company is registered for Australian customers	1 & 2	Informational (AU submissions)
C4B	Country in which the company is registered for New Zealand customers	1 & 2	Informational (NZ submissions)
C5A	For Australian customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (AU submissions)
C5B	For New Zealand customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational (NZ submissions)

6.2 Criteria – Security

Standard references are taken from:

- the Australian Government Information Security Manual June 2022 (AUISM): https://www.cyber.gov.au/ism; and
- the New Zealand Information Security Manual v3.6 (NZISM): https://www.nzism.gcsb.govt.nz/
- the Australian Privacy Principles (APP): https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/.
- the New Zealand Privacy Principles (NZPP): https://privacy.org.nz

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

In the response options column:

- the minimum acceptable response is in bold;
- the relevant assessment tier is written in brackets as a prefix to the minimum acceptable response, where "T1" means Tier 1, "T2" means Tier 2, and "T1, T2" means both Tier 1 and Tier 2. Where a country code is also provided (e.g., for control H6 – AU T1, AU T2), this indicates that this response is a minimum for that particular country only.
- a hash # (also known as an octothorpe) indicates that the question is of high importance. Failure to meet the minimum acceptable response will result in a "Non-compliant" assessment outcome.

6.2.1 Security – Product function

Q	Question	Tier	Response options	Standard
P1	Name of service	All		
P2A	Version of service *If no published version number, use date of version.*	All		
P2B	Is the service free or paid?	All	A. Free B. Paid	
P2C	For paid services, URL of pricing page	All		
P2D	Are you the product or service's original developer, a re-seller or 'other'?	All	A. Original developer B. Reseller C. Other (please specify)	
P2E	Do you warrant that you have the legal authority to submit this product or service for an ST4S assessment?	All	A. No# B. Yes (T1, T2)	
P3A	URL of service for Australian customers	All		
P3B	URL of service for New Zealand customers	All		
P4A	URL of Terms of Service/use for Australian customers	All		
P4B	URL of Terms of Service/use for New Zealand customers	All		
P5	Purpose of the service?	All		
P6	In what jurisdiction would disputes, regarding usage of the service, be handled? (e.g., Victoria Australia, New Zealand)	1 & 2		
P7	Does your organisation have a current insurance policy of at least $1M AUD with claims for data breach/loss?	1	**A. Yes - current policy with coverage of at least $1 million AUD (T1)** B. Yes - current policy but coverage is less than $1 million AUD C. No current policy	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

P8	Is this service dependent on another IT service to function according to its intended purpose? (e.g., does this service have YouTube embedded or rely on Facebook logins?) *For example, does the service utilise any third party/outsourced:* *- plug ins* *- browser extensions* *- hosting services* *- video streaming services (e.g., YouTube, Vimeo)* *- image hosting services* *- publishing services etc.*	All	A. Yes, please specify B. No	NZISM 12.7
P9	When using the service for its intended purpose, what, if any, of the data types below would reasonably be captured, stored, or processed by the service? Select all that apply. ***Sensitive information*** *is a type of personal information that is given extra protection and must be treated with additional care. If in doubt, select this option. Sensitive information may include:* *- Protection details (i.e., whether the user is under a protection order and/or the details of the order)* *- Legal custodian arrangements and court orders* *- Out of home care status* *- Records of behaviour incidents/discipline, behavioural observations/notes* *- Consent (e.g., collection and/or recording of consent)* *- Student absence details (i.e., records of attendance and reason for absence)* *- Records of contact (e.g., between parents, teacher, school, and/or student) and other agencies* *- Student/Learning support service information and support arrangements* *- Enrolment support records (sensitive case, complex case, adjustments, student plan, developmental map,*	All	•Protection order details (student) •Legal custodial arrangements (student) •Informal custodial arrangements •Legal status (criminal convictions, protection orders, police checks results etc) •Out of home care status (student) •Records of behaviour incidents (student) •Records of incidents •Behavioural observations/notes (student) •Records of contact or interview (student) •Sensitive social, emotional or mental health and well-being information (staff, student, parent) •Support arrangements (student) •Professional case notes (student) •Reason for absence (student) •Commonwealth Unique Student Identifier (AU) or National Student Number (NZ) •Health and medical details, including mental health diagnoses (staff, student, parent) •Financial information (staff, student, parent, organisation)	NZ PSR – INFOSEC1

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	transportation, Individual Education Plans, Oranga Tamariki 'All about Me' plan)		•Identification documentation (staff, student, parent) •Digital signature (staff, student, parent) •Government related Identifiers (e.g., state or federal government assigned identifiers) •Official records •Racial or ethnic origin •Religious beliefs or affiliations •Sexual orientation or practices •Biometric information (e.g., eye/retinal/facial imagery, fingerprints, biometric templates) •Location tracking data (Information about the ongoing geographic positions of individuals or devices derived from GPS or other network sources. Examples include: Current position in time and retained point in time, ongoing positions of individuals, cellular network connection tracking, BLE (Bluetooth Light Energy) beacons communication) • Use of social services (Work & Income, ACC, CYPS, Women's refuge etc) • None of the above (T2)	
P10	Select the functionality available within the service. Select all that apply.	All	• Online meetings, video or audio conferencing, livestreaming (T1) • Consent Management (T1) • Financial management or payment processing systems (T1) • Enrolment management (T1) • Student information, student management system, school administration or student administration system (T1) • Customer relationship management (T1) • Ticketing system - Service Management, Helpdesk (T1) • Learning management system (T1)	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			• Electronic document and records management systems (T1) • File hosting and synchronisation (T1) • Remote access (T1) • Data collection tools (non-curriculum) (T1) • Photo, image, video or audio storage, sharing and backup services (T1) • Two-way communication tools (T1) • Data aggregation, Data broker, Data hub, Data distribution hub (T1) • Software and cloud developer tools (T1) • Collaboration and sharing (T2) • One-way communication tools (T2) • Career education, planning and guidance (T2) • Vocational training providers and courses, industry/employment registers, work placements (T2) • Learning activities, assessments and games (T2) • Content creation, presentation tools and publishing (T2) • Educational resources and content libraries (T2) • File download, including executables (T2) • Library Management (T2) • Visitor Management (T2) • Event management, bookings, online ordering or fundraising (T2) • Administrative support services and tools (T2) • None of the above (T2)	
P11	Does the service contain, display, or promote the following via any means (social media or news feed, direct advertising, pop-ups):	All	A. Yes (please specify) **B. No (T1,T2)**	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	- Products/services: alcohol, controlled or banned substances, gambling, tobacco products, firearms and fire arm clubs, adult products and pornography. - Categories of information which may be deemed offensive by a reasonable member of the school community (e.g., racist, sexist, pornographic content etc.)			
P12	With regards to any third-party providers that make up the solution, or provide service to you, does your organisation: • have an inventory of all third-party service providers; • regularly assess and manage the risks associated with these third-party providers; and • have contractual agreements in place to ensure third-party providers adhere to your information security and privacy policies?	1	A. No B. Yes - for some third-party providers **C. Yes - for all third party-providers (T1)** **D. NA - solution does not use third party providers (T1)**	NZ PSR - GOV5 NZISM 12.7 NZPP-5 NZPP-11
P13	For the service being assessed, what is the deployment architecture used for customers?	All	A. Hosted in customer environment B. Hosted in environment owned or managed by your organisation C. Both hosted in customer environment and an environment owned or managed by your organisation	
P14	Is the service compliant with the WCAG 2.1 Accessibility guidelines as per https://www.w3.org/WAI/standards-guidelines/wcag/	All	A. No B. Yes – all components meet WCAG 2.1 AAA C. Yes – all components meet minimum of WCAG 2.1 AA **D. Yes – all components meet minimum WCAG 2.1 A (T1, T2)**	NZ Govt Web Standards
P15	Does your organisation seek to absolve indemnity from any legal liabilities with regards to the operation of the service?	1 & 2	**A. No (T1, T2)** B. Yes, outlined in publicly available terms of service or other public document or public location (please specify and provide link) C. Yes, outlined in a non-publicly available document or non-publicly available location and not actively provided to customers	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			D. Yes, outlined in a document the vendor proactively provides to all customers prior to contract phase	

6.2.2 Security – Hosting and Location

Q	Question	Tier	Response options	Standard
H1	Select the option which best describes where user data or any related data (e.g., metadata, logs, user content) is stored or processed across all components of the service, including live solution, backup, disaster recovery, test environment, and development environments.	1 & 2	**A. Entirely in a country nominated by the customer (specify supported countries for Australian and New Zealand customers) (T1, T2)** B. Entirely in a single vendor nominated country (specify country) C. In multiple vendor nominated countries: - Live solution (please specify country/s) - Other components (backup, etc) (please specify country/s)	AUISM Security Control: 1452 Revision 3 NZISM 22.1.22 NZISM 12.7 NZPP-11
H2	From what countries do vendor staff, including support, administration, development and testing, and external contractors or associates, access user data and any related data (e.g., metadata, logs) collected or used by the service (including backups and recovery)?	1 & 2	**A. Entirely from Australia and / or New Zealand (please specify)** B. From other countries (please specify country/s)	AUISM Security Control: 0975 Revision 7 NZISM 22.1.22 NZISM 12.7
H3	Retired (2022)			
H4	At a minimum, are the following physical access controls in place at the locations where data is stored: • No public access; • Visitor access only for visitors with a need to know and with a close escort; • Restricted access for authorised personnel with appropriate security clearance; • Single factor authentication for access control using secure swipe card, biometrics, coded access, other; and • Security alarm system?	1	**A. Yes – all of the above (T1)** B. Yes – some of the above C. No – none of the above	AUISM Security Control: 1296 NZISM 8
H5#	Are customers notified of any relocation or expansion (i.e. change of country) of:	1 & 2	A. No (#T1, #T2)	AUISM Security Control: 1578 Revision 0

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• the cloud infrastructure, including system components, user data and related data; and • any person (vendor or cloud infrastructure staff, external contractors or associates) with access to unencrypted customer data or any person with a means of accessing or extracting unencrypted data (e.g., those with access to encryption keys and encrypted customer data), prior to relocation?		**B. Yes (specify average notification lead time) (T1, T2)**	NZISM 22.1.22 NZISM 12.7
H6	If the service includes outsourced cloud-based services, are those cloud-based services IRAP assessed? *See https://www.cyber.gov.au/irap for information about IRAP assessment.*	1 & 2	A. No or unknown B. Yes – some outsourced cloud-based services are IRAP assessed **C. Yes – all outsourced cloud-based services are IRAP assessed (AU T1, AU T2)** **D. Not applicable – service does not include outsourced cloud-based services (AU T1, AU T2)**	AUISM Security Control: 1570 Revision 0

6.2.3 Security – Technical

Q	Question	Tier	Response options	Standard
S1#	What are the minimum encryption algorithms applied to protect all data **in transit** over networks, including encryption of data that is communicated between the user, web applications and system components (e.g., database systems)?	1 & 2	A. No encryption (#T1, #T2) B. Encryption: DES, RC4, 3DES using three distinct keys; (#T1, #T2) Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, SHA-0, SHA-1; Digital Signatures: DSA (1024) or RSA (1024); Key Exchange: DH (1024) or RSA (1024); Protocol: TLS1.1 or below **C. Encryption: AES 128 or above;** **Hashing: SHA-224 or above** **Digital Signatures: DSA (2048) FIPS 186-4, ECDSA (224+) preferably using NIST P-384 curve or RSA (1024+);** **Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve and/or RSA (2048+);**	AUISM Security Control: 1139, revision 5; ISM Security Control: 0471, revision 6; AUISM Security Control: 1277, revision 2. AUISM Security Control: 0994. NZISM 17.2 NZISM 17.3

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			Protocol: TLS 1.2 or above only(T2) D. Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+); Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)	
S2	What are the minimum encryption algorithms applied to protect data at rest, including backups, data storage and auditable logs?	1 & 2	A. No encryption B. DES, RC4, 3DES using three distinct keys C. AES 128 (T2) D. AES 192, AES 256 (AES 256 recommended) (T1) E. Encryption algorithm equivalent to options C or D (please specify equivalent algorithms)	AUISM Security Control: 0459, revision 3 NZISM 17.2
S3#	If customer data is uploaded to the service using a mechanism such as encrypted USB, SFTP, Secure API, etc., what are the minimum encryption methodologies applied?	1 & 2	A. No encryption (#T1, #T2) B. Encryption: DES, RC4, 3DES using three distinct keys; (#T1, #T2) Hashing: Message Digest (MD to MD6), RIPEMD-128 or above, Secure Hash Function (SHA-0, SHA-1); Digital Signatures: DSA (1024) RSA (1024); Key Exchange: DH (1024), RSA (1024); Protocol: TLS 1.1 or below C. Encryption: AES 128 or above; Hashing: SHA-224 or above Digital Signatures: DSA (2048) FIPS 186-4, ECDSA (224+) preferably using NIST P-384 curve or RSA (1024+); Key Exchange: DH (2048+), ECDH (256+) preferably using NIST P-384 curve and/or RSA (2048+);	AUISM Security Control: 1139, revision 5; AUISM Security Control: 0471, revision 6; AUISM Security Control: 0472, revision 6; AUSIM Security Control 1759, revision 0; AUSIM Security Control 0474, revision 6; AUSIM Security Control 1761, revision 0; NZISM 17.2 NZISM 17.3

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			Protocol: TLS 1.2 or above only(T2) D. Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+); Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1) E. N/A - Customer data is not uploaded to the service	
S4#	If multi-tenancy is used (i.e. system components are shared between multiple customers), are partitioning controls implemented to securely segregate one customer's data from another customer's data? E.g. • Assign a unique customer ID when same table is used to store multiple customers' data • Use separate table or database for each customer • Use a separate instance, environment or VPC	1 & 2	A. Yes (T1, T2) B. No (#T1, #T2) C. Not applicable	AUISM Security Control: 1436, revision 1 NZISM 10.8 NZISM 22.2
S5#	Are all of the service's web servers secured with digital certificates signed by a reputable trusted authority?	1 & 2	A. Yes (please specify CA) (T1, T2) B. No (#T1, #T2)	AUISM Security Control: 1161 NZISM 17.1 NZISM 17.2
S6	Does your organisation have a documented and implemented key management process which describes at a minimum: • Key generation; • Key registration; • Key storage;	1	A. No - none of the above B. Yes - some of the above C. Yes - all of the above (T1)	NZISM 17.9

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• Key distribution and installation; • Key use; • Key rotation; • Key backup; • Key recovery; • Key revocation; • Key suspension; and • Key destruction?			
S7#	Are production servers (e.g., authentication servers, Domain Name System (DNS), web servers, file servers and email servers), containers, serverless services and all end points protected by HIPS (Host-based Intrusion Prevention System), software-based application firewalls and anti-virus?	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above **C. Yes – all of the above except HIPS (T2)** **D. Yes - all of the above (T1)**	AUISM Security Controls: 1341, 1034, 1416, 1417 NZISM 14.1 NZISM 18.4
S8#	Does your organisation enforce the following controls on database management system (DBMS) software: • Follow vendor guidance for securing the database; • DBMS software features and stored procedures, accounts and databases that are not required are disabled or removed; • Least privileges; • File-based access controls; • Disable anonymous and default database administrator account; • Unique username and password for each database administrator account; • Use database administrator accounts for administrative tasks only; and • Segregate test and production environment?	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AUISM Security Controls: 1246, 1247, 1249, 1250, 1260, 1262, 1263, 1273 NZISM 20.4 NZISM 14.1 NZISM 10.8
S9#	Are internet facing components (e.g., web servers) separated from other online components (e.g. databases) using the following controls: • Secure communication between network segments (e.g., using firewalls), including filtering between network segments	1 & 2	A. No – none of the above (#T1) B. Partial – secure communication or DMZ C. Partial – virtual or physical network segregation (T2) **D. Yes – all of the above (T1, T2)**	AUISM Security controls: 1181, 1577, 1532, 0529, 1364, 0535, 0530, 0520, 1182, 0385, 1479, 1006, 1437, 1436, 0628 NZISM 10.8

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• DMZ for internet-facing components and separate trusted zones for other components • Virtual (e.g., VLAN) or physical network segregation			NZISM 14.1.11 NZISM 19.1 NZISM 22.2
S10#	Does your organisation have a documented and implemented system hardening process which: • Includes in scope operating systems, virtualization platforms, storage, network, applications, workstations and other end-user devices; • Includes the management of default user accounts and access levels and the uninstallation or disablement of the unnecessary services; • Ensures only required ports, protocols, services and authorisations are enabled (all others are restricted); and • Is reviewed annually and when significant changes occur?	1 & 2	A. No – none of the above (#T1, #T2) B. Yes – some of the above C. Yes – all of the above except annual review (T2) **D. Yes – all of the above (T1)**	AUISM Security Control: 1406 Revision: 2; Security Control: 1585 Revision: 0; Security Control: 1605 Revision: 0; Security Control: 1588 Revision: 0. NZISM 14.1 NZISM 22.2
S11#	Has your organisation implemented the following perimeter controls: • External Firewall; • IDS/IPS (Intrusion Detection System/Intrusion Prevention System); • DMZ (Demilitarised Zone) for hosting external sites; • Content filtering (including blocking of unnecessary file types); • DoS/DDoS (Denial of Service/Distributed Denial of Service) defence; • Web Application Firewall (WAF); • Filtering and monitoring of outgoing traffic (spikes, unusual activity, malicious content); • Network segmentation; • VPN required for remote access;	1 & 2	A. No - none of the above (#T1, #T2) B. Yes - some of the above **C. Yes - all of the above except for Web Application Firewall (WAF) (T2)** **D. Yes - all of the above (T1)**	AUISM Security Control: 1528 Revision: 1; Security Control: 1435; Revision: 1. NZISM 10.8 NZISM 18.4 NZISM 19.1 NZISM 19.3

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• Detection and monitoring of unauthorised devices on the network; • DNS filtering and network URL based filters; and • Organisation assets are configured to use trusted DNS servers?			
S12	Has your organisation documented and implemented a security policy governing the management of mobile devices, including use of a Mobile Device Management solution applied to all mobile devices?	1 & 2	A. No - none of the above (T2) B. Policy documented and implemented, but MDM not applied to all devices (T2) **C. Yes - all of the above (T1)**	NZISM 21.1 NZISM 21.4
S13#	Is production data used in non-production (e.g., test and development) environments?	1 & 2	A. Yes – without identical security controls applied and de-identification of production data. (#T1, #T2) B. Yes - with identical security controls applied and/or with production data de-identified (T1, T2) **C. No (T1, T2)**	AUISM Security Control: 1420 Revision: 2. NZISM 14.4 NZISM 20.1

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

S14	Does your organisation: - disable the internal use of business productivity tool macros (e.g., Microsoft Office macros) and scripts (VB, java, PowerShell) for users that don't have a demonstrated business requirement; - block macros in files originating from the internet; - enable macro antivirus scanning; and - ensure macro security settings can't be changed by users?	1 & 2	A. No B. Yes – some of the above **C. Yes – all of the above (T1, T2)** **D. N/A (T1, T2)**	AUISM Security Controls: 1487, 1488, 1489 NZISM 20.3

6.2.4 Security – Logging

Q	Question	Tier	Response options	Standard
L1	Does your organisation have a documented and implemented logging procedure which requires all systems in your organisation (e.g., servers, storage, network, applications, etc.) to log the following and synchronise logs to a consistent time source: • Authentication logs (e.g., successful login, unsuccessful login, logoff) • Privileged operations logs (e.g., access to logs, changes to configurations or policy, failed attempts to access data and resources) • User administration logs (e.g., addition/ removal of users, changes to accounts, password changes) • System logs (e.g., system shutdown/ restarts, application crashes and error messages)	1 & 2	A. No - none of the above B. Yes - some of the above (T2) **C. Yes - all of the above (T1)**	AUISM Security Controls: 0584, 0585, 0582, 1536, 1537 NZISM 16.6

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

L2	Does your organisation have a documented and implemented event log auditing procedure which outlines, at a minimum: • Schedule of audits (annual or real-time for sensitive data); • Definitions of security violations; • Actions to be taken when violations are detected; and • Reporting requirements?	1 & 2	A. No **B. Yes - all of the above without real-time monitoring (T2)** **C. Yes - all of the above with real-time monitoring (T1)**	AUISM Security Control: 0109 NZISM 7.1.7 NZISM 16.6
L3	Will you supply all relevant audit and logging data in response to customer requests?	1 & 2	A. No **B. Yes (T1, T2)**	
L4	Has your organisation implemented a centralised logging facility to store logs?	1	A. No **B. Yes (T1)**	AUISM Security Control: 1405 NZISM 16.6 NZISM 18.4.12

6.2.5 Security – Access

Q	Question	Tier	Response options	Standard
A1#	Are all users (including administrators), uniquely identifiable within the service (i.e., via unique usernames and passwords)?	1 & 2	A. No (#T1, #T2) **B. Yes (T1, T2)**	AUISM Security Control: 0414 NZISM 16.1
A2#	Are all passwords used to access the service (i.e. user, system, and privileged account passwords) protected in line with the recommendations of at least one of: the Australia Cyber Security Centre Information Security Manual; New Zealand Information Security Manual and/or Open Web Application Security Program's Application Security Verification Standard V2.4 Credential Storage Requirements, including the recommendation for ensuring passwords are hashed, salted and stretched?	1 & 2	A. No (#T1, #T2) **B. Yes for all users – excluding students (T1, T2). Please detail why this exception is required and specify any controls in place for student accounts.** **C. Yes for all users (T1, T2)**	AUISM Security Control: 1252 NZISM 16.1 NZISM 16.1.41
A3	At a minimum, are the following password requirements enforced for vendor staff, external contractors or associates with access to the organisation's systems and the service: • if using single factor authentication, passwords are a minimum of 14 characters with controls that limit predictability (inc. complexity)	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Control: 0421, 1559 NZISM 16.1

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• if using multi-factor authentication, passwords are a minimum of six characters			
A4	Within the service, do you offer multi-factor authentication for end-users?	1	A. No **B. Yes, offered as an option (T1)** **C. Yes, mandated for end users (T1)**	AUISM Security Control: 0974 NZISM 16.1 NZISM 21.4.11
A5#	Does your organisation **mandate** two factor authentication for: • Vendor staff, external contractors or associates accessing systems remotely; • System administrators; • Support staff; and • Staff with privileged accounts?	1 & 2	A. No – none of the above (#T1) B. Yes – some of the above (#T1) **C. Yes – all of the above (T1, T2)**	AUISM Security Control: 1173 Revision 3 NZISM 16.4 NZISM 16.7 NZISM 19.1.20 NZISM 21.4.11
A6#	Does your organisation provide access to systems based on roles (e.g., role-based access control (RBAC)), and is this process documented for all systems including the service?	1 & 2	A. No (#T1) B. Yes, for some systems **C. Yes, for all systems (T1, T2)**	NZISM 16.2 NZISM 16.4
A7#	At a minimum, are vendor staff, external contractors or associates with access to systems, applications and information (including audit logs): • Validated and approved by appropriate personnel; • Periodically reviewed (at least annually) and revalidated or revoked; and • Reviewed and revalidated or revoked following changes to role, employment and/or inactivity?	1 & 2	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Controls: 0405, 0430, 1404 NZISM 16.3 NZISM 16.5
A8	Do your support staff **require** remote access to end user devices?	1 & 2	A. Yes (please specify) **B. No (T1, T2)**	
A9	Are vendor staff, external contractors or associates with non-privileged accounts restricted from installing, uninstalling, disabling or making any changes to software and system configuration on servers and endpoints?	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Control: 1503 NZISM 14.1
A10#	Are all internal organisation systems configured with a session or screen lock that:	1 & 2	A. No (#T1) B. Yes, some of the above	AUISM Security Control: 0428

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• activates after a maximum of 15 minutes of user inactivity or if manually activated by the user; • completely conceals all information on the screen; • ensures that the screen does not enter a power saving state before the screen or session lock is activated; • requires the user to reauthenticate to unlock the system; and • denies users the ability to disable the session or screen locking mechanism?		**C. Yes, all of the above (T1, T2)**	NZISM 16.1.45
A11#	When a password reset is requested by the user, are: • the newly assigned passwords (e.g., temporary initial passwords) randomly generated; • users required to provide verification of their identity (e.g., answering a set of challenge-response questions); • new passwords provided via a secure communication channel or split into parts; and • users required to change their assigned temporary password on first use?	1 & 2	A. No (#T1) B. Yes, some of the above **C. Yes, all of the above (T1, T2)**	AUISM Security Controls: 1227, 1593, 1594, 1595 NZISM 16.1.41 NZISM 16.1.42
A12	Does the service allow user registration or logon/authentication or Single Sign-on (SSO) via credentials provided by another Identity Provider (IDP) such as RealMe, Facebook, Google, Microsoft etc.	1 & 2	A. Yes (please specify). B. No (T1, T2)	
A13#	What is the service's approach to default user access permissions (e.g., all access is denied unless specifically allowed, all access is allowed unless specifically denied)?	1 & 2	**A.** Protection by exception (Allow access unless specifically denied) (#T1, #T2) B. **Protection by default (Deny unless approved) (T1, T2)**	
A14	Does the service support Single Sign-On (SSO)?	1 & 2	A. No B. Yes – Optional. Please specify SSO supported.	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			C. Yes – Mandatory. Please specify SSO supported.	
A15	If customers can or are required to supply data to the service, what methods or mechanisms are available to support this?	1 & 2	Select all that apply: A. Flat file upload (e.g., CSV, XLS) B. API C. Creation of account in third party service for direct access to the data source D. Other (please specify) E. Not applicable	
A16A	Does the service require, suggest or imply that accounts be created in any third-party services for any purpose whatsoever (data collection, data exchange, other)?	1 & 2	A. No B. Yes	
A16B #	In relation to the creation of accounts in third party services, are enforceable written agreements in place with all of these third-party services covering this arrangement?	1 & 2 Conditional (A15 – yes)	A. No (#T1, #T2) **B. Yes (T1, T2)**	
A16C	Who creates the account/s in the third-party service?	1 & 2 Conditional (A15 – yes)	A. The school, school system or jurisdiction B. The third-party service C. The service (responding to this assessment)	
A17	Within the vendor organisation, is application control: • Implemented on all workstations; • Implemented on internet-facing and non-internet facing servers; • Enabled to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set; • Enabled to restrict the execution of drivers to an organisation-approved set;	1 & 2	A. No, none of the above B. Yes, some of the above **C. Yes, all of the above (T1, T2)**	AUISM Security Controls: 0843, 1490, 1656, 1657, 1658, 0955, 1582, 1471 NZISM 14.2

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• Implemented using cryptographic hash rules, publisher certificate rules or path rules; • Rulesets are validated on an annual or more frequent basis; and • When implementing application control using publisher certificate rules, both publisher names and product names are used.			

6.2.6 Security – HR

Q	Question	Tier	Response options	Standard
HR1#	Do all vendor staff, external contractors and associates who have access to user data or user content undergo employment screening (e.g., criminal history checks, working with children checks) as per applicable regulatory requirements?	1	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Control: 0434 NZ PSR PERSEC1
HR2#	Does your organisation run a security, privacy and online safety awareness/education program for your staff which addresses the following at a minimum: • Identification of who the awareness training needs to be delivered to; • Identification of when awareness training needs to be delivered (e.g., during induction, annually, etc.); • Identification of how the awareness training is to be delivered (e.g., classroom training, online course, security awareness posters, emails, etc.); and • The content to be delivered for each awareness session such as: o Basic understanding of the need for information security, privacy and online safety; o Actions to maintain security, privacy and online safety; o Actions to respond to suspected security, privacy and online safety incidents;	1 & 2	A. No - none of the above (#T1) B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AU ISM Security Control: 0252 NZISM 9.1 NZISM 3.2.18 NZISM 3.3.13 NZISM 7.1.7

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	o Applicable policies and laws; and o Practical security, privacy and online safety awareness exercises? o Disciplinary actions for significant security and privacy breaches by staff?			
HR3#	Is there a documented and implemented process to remove access to systems, applications and data repositories for personnel (vendor staff, external contractors and associates) that: • no longer have a legitimate requirement for access (implemented on the same day); and • are detected undertaking malicious activities (implemented immediately)?	1 & 2	A. No (#T1, #T2) B. Yes – but not implemented within required timeframes **C. Yes – (T1, T2)**	AUISM Security Control: 0430, 1591 NZISM 16.1.46 NZISM 16.4.33

6.2.7 Security – Processes and Testing

Q	Question	Tier	Response options	Standard
T1#	Does your organisation have an implemented continuous monitoring plan for all organisational systems and infrastructure that includes: • conducting vulnerability scans for systems at least monthly • conducting penetration tests for systems after a major change or at least annually • analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls • using a risk-based approach to prioritise the implementation of identified mitigations.	1 & 2	A. No (#T1, #T2) B. Yes - meets all of the requirements above but conducted less frequently **C. Yes - meets all requirements above (T1, T2)** **D. Yes – meets all requirements above including the use of external independent resources to conduct penetration testing (T1, T2)**	AUISM Security Control: 1163 NZISM 4.1.26-29 NZISM 4.3 NZISM 6.1-6.2 NZISM 14.4-14.5

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

T2#	Does your organisation use a centrally managed approach to patch or update applications, drivers, operating systems, and firmware which includes ensuring: - the integrity and authenticity of patches; - successful application of patches; and - that patches remain in place?	1 & 2	A. No – none of the above (#T1) B. Yes – some of the above **C. Yes – all of the above (T1, T2)**	AUISM Security Controls: 0298 revision 7, 0303, 1499, 1497, 1500. NZISM 12.4 NZISM 14.5.8
T3#	Are patches, updates or vendor mitigations for security vulnerabilities in: - internet facing services (including operating systems of internet-facing services); - workstation, server and network device operating systems; - operating systems of other ICT equipment; and - drivers and firmware; applied within two weeks of release, or within 48 hours if an exploit exists?	1	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Controls: 1690, 1694, 1695, 1696, 1751, 1697 NZISM 12.4
T4	Are patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products applied within two weeks of release, or within 48 hours if an exploit exists?	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Control: 1691, 1692 NZISM 12.4
T5	Are patches, updates or vendor mitigations for security vulnerabilities in other applications applied within one month of release?	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Controls: 1693 NZISM 12.4
T6#	Does your organisation have a formal, documented and implemented incident response plan which requires security, privacy and online safety incidents to be: • Investigated; • Remediated; and	1 & 2	A. No - none of the above (#T1, #T2) **B. Yes - some of the above (T2)** **C. Yes - all of the above (T1)**	AUISM Security Control: 0125 NZISM 7 NZISM 5.6 NZISM 22.1.25

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• Recorded in a register with the following information at a minimum: o Date incident occurred; o Date incident discovered; o Description of the incident; o Actions taken in response to the incident; and o Name of person to whom the incident was reported?			
T7#	When a data breach occurs, are affected customers and/or organisations notified as soon as possible after a data breach is discovered and given all relevant details (including affected individuals and what information was disclosed)?	1 & 2	A. No (#T1, #T2) **B. Yes (T1, T2)**	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5 NZISM 7.2.22 NZPP
T8	When a data loss/corruption event occurs, are affected customers and/or organisations notified as soon as possible after this is discovered and given all relevant details?	1 & 2	A. No – none of the above **B. Yes – some of the above (T2)** **C. Yes – all of the above (T1, T2)**	AUISM Security Controls: 0123, 0141, 0140 NZISM 7.2 NZPP-5

6.2.8 Security – Plans and Quality

Q	Question	Tier	Response options	Standard
Q1	(Question removed from 2021.1)			
Q2	Does your organisation have a documented and implemented Business Continuity Plan for the service which includes: • Backup strategies (including automated backups and backups that are stored disconnected); • Restoration strategies (e.g., disaster recovery); and • Preservation strategies?	1	A. No B. Yes - meets some requirements **C. Yes - meets all requirements (T1)**	AUISM Security Controls: 1547, 1548, 1510 NZISM 6.4
Q3	Does your organisation have a documented and implemented IT Change management process and supporting procedures which includes the following at a minimum: • Applicable criteria for entry to and exit from the change management process	1 & 2	A. No change management process B. Yes, change management process meets some requirements **C. Yes, change management process meets all requirements (T1, T2)**	AUISM Security Control: 1211 NZISM 6.3

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• Categorisation of IT change (e.g., Standard, Pre-Approved, Emergency, etc.); • Approval requirements for each category of IT change; • Assessment of potential security impacts; • Prerequisites for the IT change (e.g., the IT change has been tested in a non-production environment); • Documentation requirements in regard to the change (e.g., completion of a template in an IT change management tool, completion of a rollback plan, etc.); • Documentation that needs to be updated as a result of the change (e.g., as-built documentation, IT Disaster Recovery Plans, etc.); and • IT change communication processes (e.g., notifications to users)?			
Q4	Does your organisation have a documented and implemented security, privacy and online safety risk management framework and supporting processes, which outlines at a minimum: • Scope and categorisation of information assets and systems; • Identification and assessment of risks/ threats, including those relating to the supply chain (e.g. from outsourced services that the solution relies on); • Selected and implemented controls to manage risks with the following details recorded in a risk register: o Identified security risks, categories and risk ratings; o Risk owner(s); o Mitigation actions; o Accepted risks (where applicable) and; o Residual risk ratings after implementing mitigation actions • Proactive monitoring and testing of information assets and systems to maintain the security posture on an ongoing basis?	1 & 2	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AUISM Security Control: 1636, revision 0, ISM Security Control: 1526, revision 1 NZISM 3.2.10-13 NZISM 3.3.5-8 NZISM 4.1

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Q5#	Are all service application developments assessed as per a security testing methodology that is consistent with the guidance provided by the latest industry standard frameworks (e.g., Open Web Application Security Project (OWASP) Testing Guide v4.2, Building Security In Maturity Model (BSIMM))?	1 & 2	A. No (#T1, #T2) B. Yes - security testing partially satisfies the guidance provided in an industry standard framework (please specify framework) **C. Yes - security testing fully satisfies the guidance provided in an industry standard framework (T1, T2) (please specify framework)**	AUISM Security Control: 1239 NZISM 14.4.6 NZISM 14.5.8
Q6	Does your organisation have a documented and implemented IT Asset management process including: • A register of all components that make up the service, including software, databases, middleware, infrastructure etc (their version numbers, patch levels and configuration); • An ICT equipment and media register that is maintained and regularly audited; • A directive that ICT equipment and media are secured when not in use; • The secure disposal of ICT equipment and media (including sanitising/removal of any data or secure destruction/shredding)?	1	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	AUISM Security Control: 0336, revision 4, ISM Security Control: 0159, revision 4 NZISM 8.4 NZISM 12.6 NZISM 13.4-13.6
Q7	Does your organisation have a documented and implemented information security policy that outlines the following at a minimum: • management direction and support for information security; • requirement to comply with applicable laws and regulations; • information security roles and corresponding responsibilities/accountabilities; and • requirement for communication to management to ensure they maintain an awareness of, and focus on, addressing privacy and security issues?	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Control: 1478 revision 1. NZISM 5.1.7 NZISM 5.2
Q8	Does the service's application development have the following characteristics:	1 & 2	A. No – none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	NZISM 14.4 NZISM 14.5

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• Environments are separated into at least development, testing and production environments; • Development and modification of software only takes place in development environments; • Unauthorised access to the authoritative software source is prevented; • Secure-by-design principles and secure programming practices are used as part of application development; • Privacy-by-design principles; and • Threat modelling is used in support of application development?			

6.2.9 Security – Incidents

Q	Question	Tier	Response options	Standard
I1	Has the organisation, platform, or service had a recent security and/or privacy incident or breach?	1 & 2	A. Yes – less than 12 months ago **B. Yes – greater than 12 months ago (T1, T2)** **C. No (T1, T2)**	

6.2.10 Security – Data Deletion and Retention

Q	Question	Tier	Response options	Standard
D1	Are all data backups stored for a minimum of 3 months?	1 & 2	A. No **B. Yes (T1, T2)**	AUISM Security Control: 1514 NZISM 6.4
D2	Is deletion of customer data certified?	1 & 2	A. No B. Yes, but certificate not provided to customer **C. Yes, with certificate provided to customer upon request (T1)**	NZISM 13.1 NZISM 13.4-13.6 NZISM 22.1.26
D3#	Is the full restoration of backups tested at least once when initially implemented and each time major information technology infrastructure changes occur, or at least annually? (e.g., technology stack changes, vendor changes, platform changes)?	1 & 2	A. No (#T1, #T2) **B. Yes (T1, T2)**	AUISM Security Control: 1515 NZISM 6.4

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

D4#	Is the partial restoration of backups tested on a quarterly or more frequent basis?	1 & 2	A. No (#T1) **B. Yes (T1, T2)**	AUISM Security Control: 1516 NZISM 6.4

6.2.11 Security – Compliance Controls

Q	Question	Tier	Response options	Standard
CC1	Select the compliance certifications or security assessments that have been completed for the service and your organisation, or another organisation contracted by you to perform the development, maintenance and/or support of your solution (excluding the infrastructure provider e.g., AWS, Azure, Sendgrid)	1 & 2	A. ISO/IEC27001 B. SOC 2 Type II C. FEDRAMP (NIST) D. IRAP E. Privacy confirmation (GDPR, SOPAA, Privacy Shield) F. Cloud Security Alliance STAR G. Cloud Vendor Assessment Tool (HECVAT) H. Other (please specify) I. None of the above	NZISM 5.8 NZ PSR – INFOSEC3, GOV8
CC2#	If the solution processes electronic payments or holds credit card data is it Payment Card Industry Data Security Standards (PCI DSS) compliant?	1 & 2	A. No (#T1, #T2) **B. Yes – service is PCI compliant (T1, T2)** **C. Yes – outsourced to PCI compliant third party (please specify) (T1, T2)** **D. N/A – Solution does not process payments or hold credit card data (T1, T2)**	NZISM 5.8

6.2.12 Security – Governance

Q	Question	Tier	Response options	Standard
G01	Is there a nominated role within the organisation responsible for information security (i.e., CIO, CTO, CISO)?	1 & 2	A. No **B. Yes (T1, T2) (Please specify role title)**	AUISM 0714 NZISM 3.2
G02	Is there a nominated role within the organisation responsible for privacy (i.e., CIO, CTO, CISO, Privacy Officer)?	1 & 2	A. No **B. Yes (T1, T2) (Please specify role title).**	NZPP
G03	Has responsibility for and ownership and accountability of critical system assets been assigned to individual/s in the organisation?	1 & 2	A. No **B. Yes (T1, T2)**	NZISM 3.4

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

G04	What countries are your organisation's security and privacy operations teams and real-time monitoring and incident response systems located?	1 & 2	**A. Entirely within Australia and/or New Zealand (please specify) (T1, T2)** B. From other countries (please specify country/s) C. No defined security and privacy operations teams	

6.3 Criteria – Privacy

6.3.1 Privacy

Q	Question	Tier	Response options	Standard
PA1	Are the terms of service/use made available free of charge, and, **published on the internet or provided to customers prior to use of the service?**	1 & 2	A. No B. Yes **(T1, T2)**	
PA2	As per the terms of service, what, if any, age restrictions apply to the use of the service?	1 & 2	A. Users must be over the age of 18 B. Users under the age of 18 can use the service with parent/guardian consent **C. No age restrictions apply (T1, T2)** D. Other (please specify) **E. NA - this service will not be used by students (T1, T2)**	
PA3	What are the specified definitions of intellectual property ownership, including copyright, in the terms of use for the service? (e.g., user generated content)? Include excerpt from terms of use.	1 & 2	A. Not specified B. Service provider has ownership or unrestricted licence to copy, alter, distribute, perform, display to all other users, third parties, affiliated organisations, etc. The service provider notifies users if their intellectual property is used for any of these purposes. C. Service provider has ownership or unrestricted licence to copy, alter, distribute, perform, display to all other users, third	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			parties, affiliated organisations etc. The service provider does not notify users if their intellectual property is used for any of these purposes. **D. User retains intellectual property rights to their own work created within and/or uploaded to the service (T1, T2)**	
PA4	As per the terms of service, are users forewarned in the event the service provider wishes to terminate their account?	1 & 2	A. No **B. Yes (T1, T2)** **C. N/A - Service provider does not terminate accounts (T1, T2)**	

6.3.2 Privacy – Requests

Q	Question	Tier	Response options	Standard
PR1#	Is the privacy policy **made available free of charge, and:** • Published on the internet; or • Provided to customers prior to use of the service?	1 & 2	A. No (#T1, #T2) **B. Yes (T1, T2)**	APP: 1.5 NZPP-3
PR1A	Enter the URL for the service's Privacy Policy or upload the Privacy Policy document	1 & 2		NZPP-3
PR2#	Does the privacy policy for the service outline the following requirements about the collection and management of personal information at a minimum: • The kinds of personal information that the entity collects and holds; • How the entity collects and holds personal information; • The purposes for which the entity collects, holds, uses and discloses personal information; • How an individual may access personal information about the individual that is held by the entity and seek the correction of such information; • How an individual may complain about a breach of their privacy, and how the entity will deal with such a complaint; • Whether the entity is likely to disclose personal information to overseas recipients; and	1 & 2	A. No (#T1, #T2) B. Yes - includes some of the above (#T1, #T2) **C. Yes - includes all of the above (T1, T2)**	APP: 1.4 NZPP-3 NZPP-6 NZPP-7

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy?			
PR3A	What **mandatory** information is collected by the service when **school staff** generate their own accounts for this service? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I Country or state/province J. Role (for school leaders) K. Evidence of identity L. Other (please specify): M. N/A - school staff do not register their own accounts for this service	NZPP-3
PR3B	What **mandatory** information is collected by the service when **students** generate their own accounts for this service? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Role (for school leaders) K. Evidence of identity L. Other (please specify): M. N/A - students do not register accounts for this service	NZPP-3

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			N. N/A - students do not register their own accounts for this service	
PR3C	What **mandatory** information is collected by the service when **parents** generate their own accounts for this service? Select all that apply. If not required, select N/A. NOTE: *This question relates to when parent accounts are required for school use of the service. If parent accounts are not required, select, "N/A parent accounts are not required for school use of this service".*	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - parent accounts are not required for school use of this service M. N/A - parents do not register their own accounts for this service	NZPP-3
PR4A	What **mandatory** information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of school **staff**? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school-based administrators or teachers or the service provider cannot generate accounts on behalf of staff	NZPP-3

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

PR4B	What **mandatory** information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of **students**? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of students	
PR4C	What **mandatory** information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of **parents**? Select all that apply. If not required, select N/A.	1 & 2	A. Title B. First name C. Surname D. Email address E. Gender F. Date of birth (i.e., dd/mm/yy) G. Age, month and year of birth, or year of birth H. Year level I. Country or state/province J. Evidence of identity K. Other (please specify): L. N/A - school based-administrators, teachers or the service provider cannot generate accounts on behalf of parents	
PR5	Do the terms of use for the service require complete and accurate information to be entered when registering accounts for the service (e.g., are the use of pseudonyms or de-identified information not permitted)? Please include excerpt from the terms of service.	1 & 2	A. Yes (please include excerpt from the terms of service) **B. No (T1, T2)**	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

PR6	Are customers/users offered anonymity and/or pseudonymity when dealing with the service provider in some circumstances (e.g., providing feedback)?	1 & 2	A. No **B. Yes, please specify circumstances (T1, T2)**	APP: 2.1 NZPP-1
PR7	Are mandatory fields clearly distinguished from optional fields during the standard account registration process?	1 & 2	A. No **B. Yes (T1, T2)**	NZPP-3
PR8	Are mandatory fields clearly distinguished from optional fields when schools, teachers, or the service register accounts on behalf of other users (e.g., students, staff, or parents)?	1 & 2	A. No **B. Yes (T1, T2)**	NZPP-3
PR9	If unsolicited personal information is provided to the service (e.g., when existing customer data is uploaded to the service), is the information destroyed or de-identified as soon as practicable if it is lawful to do so?	1 & 2	A. No **B. Yes (T1, T2)**	NZPP-9
PR10#	Does your organisation share user data with third parties in any circumstance other than the following? If yes, please specify. -the individual has consented to the use or disclosure of the information; -the use or disclosure of the information is required or authorised by or under a law or a court/tribunal order in the customer's country; - the use or disclosure is required or permitted under privacy legislation in the customer's country; or -the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body? For service in Australia, refer to the Australian Privacy Principles, as well as the permitted general situations and permitted health situations. For service in New Zealand, refer to the Privacy Principles and information sharing provisions in the Privacy Act 2020,	1 & 2	A. Yes (please specify) (#T1, #T2) **B. No (T1, T2)**	APP: 6.1, 6.2 NZPP-11

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	as well as the Oranga Tamariki Act 1989 and the Family Violence Act 2018.			
PR11	Can users opt-in or opt-out to the service's commercial mailing list/promotional/marketing communications (e.g. email mailing lists)? *Commercial mailing lists are those that are used for the purpose of distributing sales and marketing and promotional materials, including (but not limited to) competitions, education research related to the product, and end user feedback.* *Commercial mailing lists do not include lists used for the purpose of sending important service information, such as notifications of service disruption, data breach or loss; upgrade notifications; and subscription renewals.*	1 & 2	A. Users cannot opt-out. Users are automatically subscribed to receive commercial/promotional/marketing communications. B. Users can opt-out. Some or all users are automatically subscribed but can opt-out after the fact **C. Users can opt-in. Users do not receive commercial/promotional/marketing communications unless they explicitly opt-in (T1, T2)** **D. N/A – The service or organisation does not have any commercial/promotional/marketing communications (T1, T2)**	
PR12#	Does the service adopt government related identifiers of individuals as its own identifier of the individual or use or disclose government related identifiers for any reasons other than the list below: • The government related identifier is required or authorised by or under a law or a court/tribunal order within the customer's country; • Use or disclosure is necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; • Use or disclosure is necessary for the organisation to fulfil its obligations to a government agency or education authority within the customer's country;	1 & 2	A. Yes (provide details of the identifier(s) and how each is used) (#T1, #T2) **B. No (T1, T2)**	APP: 9.1, 9.2 NZPP-13

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• Use or disclosure is required or authorised by or under a law or a court/tribunal order within the customer's country; • The organisation reasonably believes the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities; • The identifier, organisation or circumstances are prescribed by regulations?			
PR13#	Does your organisation have a process which allows customers to request the service to provide access to, correct, or delete all personal information relating to them?	1 & 2	A. No (#T1, #T2) B. Yes - with a cost and resolved outside of 3 months C. Yes - with a cost and resolved within 3 months **D. Yes - free of charge and resolved outside of 3 months (T2)** **E. Yes - free of charge and resolved within 3 months (T1, T2)** F. NA - service does not collect personal information **(T1, T2)**	APP: 12.1, 13.1 NZPP-6 NZPP-7
PR14#	Does the service provide any discovery functionality which allows users from one school to find, access or discover users or personal information from another school, or organisation? Examples include enabled searching (by user, user details or resources), or data sharing (e.g. to support student transfer) or integration (e.g. for analytics) between customers (e.g. different schools). Select all that apply.		A. No discovery functionality exists within service (T1,T2) B. Discovery functionality can be restricted to the user's current school/year level/class C. Discovery functionality is disabled by default D. An administrator can restrict discovery functionality at the user level (i.e. allow some but not all users access discovery functionality) E. Discovery is possible, but none of the controls above are available (#T1, #T2)	NZPP-11
PR15	Does the service capture a user's location data?		A. No, user location data not required. (T1, T2) B. The service must capture user location data to function. Location data is captured with a user's explicit consent (T1, T2)	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			C. The service must capture user location data to function. Location data is captured without a user's explicit consent. D. The service does not require user location data to function, but does capture it with a user's explicit consent. E. The service does not require user location data to function, but does capture it without a user's explicit consent.	

6.3.3 Privacy – Functionality

Please note: Functionality questions allow us to better understand how given functionality works and what controls are available. Generally speaking, an ability to disable, restrict access to, or moderate functionality will result in a lower risk level.

Q	Question	Tier	Response options	Standard
PF1	When using the service, are users under the age of 18 exposed to advertising and/or offers?	All	A. Yes **B. No (T1, T2)**	
PF2	Does the service provide functionality that allows school-based administrator accounts to control role-based access for school users (e.g., staff or students) in order to restrict access to stored information and/or functionality within the system?	**1 & 2**	A. No **B. Yes, please provide details (T1, T2)** **C. N/A (T1, T2)**	
PF3	Does the registration of an account or use of the service generate a user 'profile' within the service, and if so, can visibility be restricted (e.g., made private or restricted to known users)?	1 & 2	A. Profile is generated, but user or administrator cannot restrict visibility of their profile B. Profile is generated, and user or administrator can restrict visibility of their profile **C. Profile is generated but only visible to user (e.g., visibility is restricted by default) (T1, T2)** **D. No user profile is generated (T1, T2)**	
PF4	Select all functionality available within the service.	All	Informational only, used to generate subsequent questions.	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			A. Forms, surveys and eSignatures B. Online meetings, video conferencing, audio conferencing C. Remote access tools D. Screen Sharing E. Chat / Instant Messaging F. Commenting and communities/forums G. Quiz, poll, flashcard creation and/or distribution H. File download, including executable, developer tools, images etc. I. Direct email J. File upload and storage, and file sharing and collaboration K. Content creation and collaboration L. Content libraries M. Notifications and alerts N. Online learning activities, assessments and/or games O. Administrative support services and records management P. Data integration, aggregation, data broker, data hub, data distribution hub Q. Assessment or collection of health and well-being information including socio-emotional factors (e.g., physical and mental health, well-being, behaviour) R. Other S. None of the above	
PF5	In relation to the form, survey and/or eSignature functionality, select which features are offered within the service. Select all that apply.		A. Online forms - service provider generated, non-editable B. Online forms - customisable / editable / user generated C. Surveys - service provider generated, non-editable	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			D. Surveys - customisable / editable / user generated E. eSignatures F. Forms/surveys can be distributed and/or shared via linked social media accounts (Facebook, Twitter etc.) G. Forms/surveys can be shared as templates for re-use by others	
PF6#	In relation to the online meeting, video conference, audio conferencing and/or livestreaming functionality available within the service, select all that apply.		A. Access to sessions can be made available to the public B. Access to sessions can be made private (e.g., access to sessions is invitation only) C. Participant details can be displayed to all session participants D. Participants can be displayed with de-identified/anonymous details or kept private E. Sessions can be recorded and made available to the public F. Sessions can be recorded and made private (e.g., participants only) G. Audit logs are not kept for all recordings (#T1, #T2) H. Participants are not notified if they are participating in a recorded session (e.g., via on screen prompt) (#T1, #T2)	
PF7#	In relation to the remote access tools available within the service, select all that apply.		A. Remote access tools can be disabled by an administrator or moderator B. Remote access sessions can be initiated without the agreement of the user (#T1, #T2) C. Users cannot take back control during remote access sessions (#T1, #T2) D. Users cannot terminate remote access sessions once initiated (#T1, #T2) E. Onscreen notification is displayed throughout remote access sessions	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			F. Remote access sessions are not logged (#T1, #T2)	
PF8#	In relation to the screen sharing functionality available within the service, select all that apply.		A. Use of screen sharing functionality is disabled by default B. Screen sharing can be disabled by an administrator or moderator C. Screen sharing sessions are initiated and/or accepted by the user who is sharing their screen D. Screen sharing sessions are not logged (#T1, #T2)	
PF9#	In relation to the chat/instant messaging functionality available within the service, select all that apply.		A. Chat/instant messaging is unmoderated B. The service moderates chat/messages using a profanity filter C. The service moderates chat/instant messaging and reserves the right to remove posts and/or users that breach the Terms of Use D. Users can report chat/instant messaging that breaches the Terms of Use E. Users can chat/message with non-account holders (i.e., no log in is required to participate in chat/messaging) F. Communication can be limited to restricted groups only (e.g., class, year level) G. Chat/instant messaging can be disabled by an administrator/moderator H. Chat/instant messaging is visible to an administrator (e.g., teacher) in real time I. Chat/instant messaging is not logged (#T1, #T2) J. None of the above	
PF10#	In relation to the commenting and communities/forums functionality available within the service, select all that apply:		A. Non-account holders can post comments (i.e., no log in is required to participate in commenting)	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			B. The service applies a profanity filter prior to publishing C. The service moderates comments and reserves the right to remove posts and/or users that breach the Terms of Use D. Users can report comments that breach the service's Terms of Use E. Comments must be approved by an administrator or the service prior to publishing F. Commenting can be disabled by an administrator/moderator G. An administrator can control what users can comment on and which users can comment (e.g., a teacher can restrict students to only comment on the work of classmates) H. Commenting is unmoderated I. Comments are not logged (#T1, #T2) J. Users can upload files or share projects or files in forums/communities K. None of the above	
PF11	In relation to the quiz, poll and flashcard functionality, select which features are offered within the service. Select all that apply.		A. Quizzes - service provider generated, non-editable B. Polls - service provider generated, non-editable C. Flashcards - service provider generated, non-editable D. Quizzes - customisable / user generated E. Polls - customisable / user generated F. Flashcards - customisable / user generated G. Quizzes, polls and/or flashcards can be shared as templates for re-use by others	
PF12	(Question removed from 2021.1)			

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

PF13	In relation to the file download functionality available, select all files types that can be downloaded within the service.		A. Executable files and/or code (e.g., .exe) B. Desktop publishing files (e.g., .doc, .pdf, .ppt) C. Image files (e.g., .png, .jpg, .jpeg) D. Audio files (e.g., .mp3, .wma, .wav) E. Video files (e.g., .avi, .mov, .wmv, .gif) F. Database files (e.g., .dat, .csv, .log, .mdb) G. Other	
PF14#	At a minimum, are the following features built into the file download functionality available within the service: • All files are scanned for Malware/Viruses during download; • All files are scanned for Malware/Viruses while at rest; and • All files found to contain Malware/Viruses are deleted or quarantined?		A. None of the above (#T1, #T2, if also support download of .exe (A) or database files (F) from PF13) B. None of the above, but users cannot download files uploaded by other users C. Yes, some of the above **D Yes, all of the above (T1, T2)**	AUISM Security control: 0657 NZISM 14.1
PF15	When sending correspondence via the service on behalf of the school, how does the service send email communication to the school's recipients/audience? Select all that apply.		A. Sent from the school user's registered email address B. Sent from the service's domain (e.g., user@servicename.com) C. Sent from unverified, anonymous or invalid email addresses D. Other	
PF16	What, if any, third party products are used to provide the file upload and storage functionality within the service? Select all that apply.		A. YouTube B. Vimeo C. Flickr D. Image Shack E. Picasa F. Other image and video streaming services G. DropBox H. Google Drive I. OneDrive J. Box K. iCloud L. Other cloud storage and file sharing	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			M. No third-party products are used	
PF17	In relation to the file upload and sharing functionality available within the service, select all that apply.		A. Authors have control over who can view and/or edit their files B. Administrators (e.g., teachers) can restrict who can view and/or edit users' files C. Administrators can disable file sharing D. None of the above E. Not applicable – file sharing is not supported	
PF18#	At a minimum, are the following features built into the file upload functionality available within the service? • All files are scanned for Malware/Viruses during upload • All files are scanned for Malware/Viruses while at rest • All files found to contain Malware/Viruses are quarantined or deleted		A. None of the above (#T1, #T2) B. Yes, some of the above C. Yes, all of the above (T1, T2)	AUISM Security control: 0657 NZISM 14.1
PF19	In relation to the content creation functionality available within the service, select all that apply.		A. Users can share their content (e.g., via direct urls) B. Users have control over who can view or edit their content C. Administrators can restrict who can view and/or edit users' content D. Administrators can disable sharing of users' content E. None of the above	
PF20	Select the response option which best describes the publication of user generated content. Publication means visible to all members and/or visitors to the service.		A. User generated content can be published to the service but no privacy settings can be applied B. User generated content can be published to the service and privacy settings can be applied C. User generated content cannot be published to the service	
PF21	In relation to the content libraries available within the service, select all that apply. Content may include:		A. Educational or curriculum aligned content and activities B. Non-educational content and activities	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			C. Template libraries (e.g., presentations, web design, surveys etc.) D. Image, video and audio libraries E. Search results that are not filtered based on user characteristics (e.g., age, year level, user type etc.) F. None of the above	
PF22	Who can publish content to content libraries within this service (i.e., users or service provider); and is content subject to moderation to ensure users are not exposed to information, including images, video, text and/or recordings, which may be deemed: • Offensive by a reasonable member of the school community (e.g., nudity, pornography, graphic content, profanity, racist, sexist etc. and/or • Inappropriate for users under 18 years? Moderation may include: • The service reserves the right to remove content that breaches the Terms of Use • The service applies a profanity filter • The service has an implemented assurance procedure to ensure content conforms to quality standards prior to publication • Users can report content that breaches the Terms of Use Select all that apply.		A. Service provider generated content with moderation B. Service provider generated content without moderation C. User generated content with moderation D. User generated content without moderation	
PF23	In relation to the notification and alert functionality available within the service, select all that apply.		A. Notifications and alerts can be one-way (broadcast) B. Notifications and alerts can be two-way e.g., parents/recipients can respond to notifications and alerts C. Notifications can be via email D. Notifications can be via SMS	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			E. Notifications can be via push notifications F. Notifications and alerts can be disabled by an administrator/moderator G. For each notification and/or alert, the school and/or users can specify and/or limit the audience H. The school and/or user can create and manage a subscriber group, and only members of this group can receive notifications and/or alerts from the school and/or user	
PF24	(Question removed from 2021.1)			
PF25	In relation to the online learning activities, assessment and/or game functionality available within the service, select all that apply.		A. The service provides standardised testing B. The teacher or user can create their own online learning activities and/or games. C. Answers can include pre-defined response options (e.g., multiple choice, Likert scales etc.) D. Answers are numerical free text fields (e.g., 0-9) E. Answers are short response free text fields (e.g., typing, equations, units of measurement, spelling and vocabulary) F. Answers can include long response free text fields (e.g., sentences, paragraphs, essays etc.) G. Data analysis, analytics and/or reporting is generated H. Data analytics and/or reporting can be sent to parents via the service. I. Other	
PF26	Select the response option which best describes the publication of results on the service. Results are considered to be published if they are visible to anyone other than the owner of the results.		A. Student results can be published on the service but privacy settings cannot be applied. B. Student results can be published on the service and privacy settings can be applied. C. Student results cannot be published.	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

PF27	In relation to any other functionality that is offered by the service, select all that apply.		A. Online ordering B. Financial management or payment processing systems C. Enrolment management D. Student information, student management system, school administration or student administration system E. Customer relationship management F. Ticketing systems G. Electronic document and records management systems H. Data integration, aggregation, data broker, data hub, data distribution hub I. Library Management J. Visitor Management K. Event management, bookings, online ordering or fundraising L. Subject selection M. Class formation N. Assignment submission O. Plagiarism detection P. Roll marking Q. Absence reporting and notifications R. Timetabling S. Academic reporting T. Other U. None of the above	
PF28	What names do you, as the service provider, give to the various modules available within the service?		*Informational question- used to inform QA and data assets disclosed to service.*	
PF29	What additional student data - other than that which is mandatory to register an account - can be provided to / collected by the service when used for its intended purpose? Please indicate whether this data field is mandatory or optional.		For each indicate mandatory, optional or not collected: A. Protection details B. Legal custodian arrangements C. Out of home care status	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			D. Records of behaviour incidents E. Behavioural observations/notes F. Support arrangements G. Professional case notes H. Consent I. Attendance, including reason for absence J. Records of interview and/or contact K. Academic results L. Academic testing M. Personality profiling, career goals and/or interests N. Unique Student Identifier O. Timetabling P. Emergency contacts Q. Other R. None of the above	
PF30	What additional student, staff and/or parent data - other than that which is mandatory to register an account - can be provided to / collected by the service when used by the school for its intended purpose? This question is not intended to collect information about parent's personal use of the service (e.g., when it is not associated with school use/subscription). For each data asset, please specify whether it relates to student, staff, or parent. Select N/A if not collected.		For each indicate mandatory, optional or not collected: A. Medical details B. Well-being information C. Year level D. Class name E. School name F. Works G. Image H. Video or audio recording I. Email address J. First name K. Surname L. Date of Birth M. Age, month and year of birth, or year of birth N. Home address O. Phone number	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			P. Identification documentation Q. Electronic signature R. Cultural and citizenship details, racial or ethnic origin S. Religion T. Gender U. Languages spoken V. Username - determined by the user W. Country or State/province X. Responses - online learning, surveys, forms Y. Resume, CV, applications, references Z. Certificates and accreditation AA. User location data AB. N/A	
PF31	What, if any, other data not listed above can be disclosed to or collected by the service if used for its intended purpose? Please specify if data relates to student, staff or parent and whether it is mandatory or optional.		Free text field (informational)	
Data integration, aggregation, data broker, data hub, data distribution hub control questions (PF32, PF33, PF35, PF36, PF40-PF50)				
PF32	In relation to the data integration, aggregation, data broker, data hub, data distribution hub functionality, does the service (the collector of data/ data aggregator / data broker) assume ownership of any data transferred to, or transiting through, the service?		A. Yes **B. No (T1, T2)**	
PF33	In relation to the sharing of data with any third party (any service which receives data of any form from the service), are enforceable, written agreements in place with data suppliers or recipients that covers: • the purpose for data sharing; • the scope of data to be shared (e.g., academic results); • the scale of data sharing (e.g., current student records only, or a specific year level);		A. No B. Yes - Some of the above but data agreements not updated C. Yes - Some of the above with data agreements updated **D. Yes (T1, T2)**	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	• the security and privacy controls in place in recipient systems; and • ownership of data. Furthermore, data agreements are updated to reflect changes in any of the above?			
PF34	Retired			
PF35	Who authorises the transfer of data, including the data scope (e.g., student academic results) and scale (e.g., only year 8 students) from the service (data integration/aggregation service, data broker, data hub, data distribution hub) to recipient third party systems:		Select all that apply: **A. Data sharing can be controlled by the customer (school, school system or jurisdiction) (T1, T2)** B. Data sharing can be controlled by the data aggregator (service being assessed) C. Data sharing can be controlled by the data recipient	
PF36#	When a data breach or data loss event occurs in third party recipient systems, who notifies the customer (e.g., school, school jurisdiction or school system)?		**A. Data aggregator notifies customer as soon as possible after discovery and provides all relevant details (T1, T2).** B. Data aggregator notifies customer without commitment to timeframe and/or details not provided. C. Third party service notifies customer as soon as possible after discovery and provides all relevant details. D. Third party service notifies customer without commitment to timeframe and/or details not provided. E. Unknown (#T1, #T2) F. No notification of customer occurs (#T1, #T2)	
PF40	Does your service offer enterprise level controls (for example schools that belong to an owning higher authority (e.g. a Department or Education Authority))?	1 & 2	A. No B. Yes – two or more levels (e.g. school level controls and Departmental controls)	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			C. **Yes – two or more levels with Departmental controls overriding school level controls (T1, T2)**	
PF41	When your service ingests data from a customer's source system, does the customer have the ability to specify and restrict the exact data elements/fields (i.e. 'select' and 'where' clauses) shared with your service?	1 & 2	A. No (please specify) B. Yes - source system extract can be defined by the school only C. Yes - source system extracts can be defined by the school or higher (enterprise/departmental) authority. Higher authority settings can be altered by the school D. **Yes - source system extracts can be defined by the school or higher (enterprise/departmental) authority. Higher authority settings cannot be altered by the school (T1, T2)**	
PF42	Does your service offer the ability for the customer to restrict which recipient systems are available for integration?	1 & 2	A. No B. Yes - Recipient systems can be defined by the school only C. **Yes - Recipient systems can be defined by the school or higher (enterprise/departmental) authority and are not able to be modified schools (T1, T2)**	
PF43	Can the customer of your service restrict the data elements/fields that are shared with each individual recipient system?	1 & 2	A. No B. **Yes (please specify) (T1, T2)**	
PF44	Does your service have an administrative view that clearly shows to the customer which recipient systems your service is currently sharing customer's data with and the types of data being shared?	1 & 2	A. No B. **Yes (T1, T2)**	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

PF45	Does your service require customers to regularly reauthorize all recipient and integrating systems and perform a review of all data elements/fields shared?	1 & 2	A. No **B. Yes (please describe the process including frequency) (T1, T2)**	
PF46	Does your service offer the ability to filter and thereby prevent, exclude or limit the collection or handling of a specific individual's information or their related data?	1 & 2	A. No B. Yes - filtering can be applied only **after** source data is consumed by your service. Filtered records are then not shared with recipient systems (please describe) (This response triggers the below risk and treatment) **C. Yes - filtering can be applied prior to data being consumed by your service (T1, T2) (please describe)** D. Yes – other (please describe)	
PF47	When a customer withdraws data sharing approval for a recipient system what action does your service take?	1 & 2	A. The service immediately suspends all data sharing with the recipient system. B. The service notifies the recipient system of the withdrawal of approval. C. The service purges all data within the service it holds related to the recipient system. **D. All of the above (T1, T2)** E. None of the above.	
PF48	Does your service support the two-way flow of data i.e. data can be sent to a recipient system AND data can be returned from the recipient system to your service for write-back to customer systems?	1 & 2	A. No **B. Yes. Please specify which systems and data are supported for write-back from your service. (T1, T2)**	
PF49	Prior to onboarding a recipient system to your service, what due diligence checks and verifications are performed by your organisation on recipient systems?	1 & 2	A. Security check performed or evidence of security maturity obtained (please specify including details of any	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			industry standard or other certifications) B. Privacy check performed or evidence of privacy maturity obtained (please specify including details of any industry standard or other certifications) C. Security and privacy requirements are detailed in contracts between the service's organisation and the recipient system **D. All of the above (T1, T2)** E. None of the above.	
PF50	Are ongoing checks and monitoring performed by your organisation on the service's recipient systems to ensure compliance with security and privacy requirements?	1 & 2	**A. Yes (please detail and specify frequency) (T1, T2)** B. No	
PF37	In relation to the assessment or collection of health and well-being information through functionality available within the service, select all that apply:		A. Online forms – service provider generated, non-editable B. Surveys – service provider generated, non-editable C. Quizzes – service provider generated, non-editable D. Polls – service provider generated, non-editable E. Learning activities and/or game-based assessment F. Diagnostic and/or standardised testing G. Online forms – customisable / user generated H. Surveys – customisable / user generated I. Quizzes – customisable / user generated J. Polls – customisable / user generated	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			K. Learning activities and/or game-based assessment – customisable / user generated N. Data analysis, analytics and/or reporting is generated for users based on their responses P. Well-being data analytics and/or reporting can be sent to parents via the service. Q. In-built monitoring and/or reporting tools identify respondents who may require follow-up or additional support. R. No in-built monitoring and/or reporting tools are provided to identify respondents who may require follow-up or additional support.	
PF38	In relation to the response options available within the service to assess or collect health and well-being information, select all that apply:		A. Responses can include pre-defined response options (e.g., multiple choice, Likert scales etc.) B. Responses are numerical free text fields (e.g., 0-9) C. Responses are short response free text fields (e.g., typing, equations, units of measurement, spelling, and vocabulary) D. Responses can include long response free text fields (e.g., sentences, paragraphs, essays etc.) E. Users can request further assistance or to talk to someone. F. Users can request further assistance or to talk to someone and this automatically notifies the school-nominated staff member. G. Users are de-identified and response data is aggregated/summarised so users and respondent data and reports are anonymous. H. Response data is aggregated/summarised so respondent data and reports do not identify the user.	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

			I. Respondent data and reports identify individuals for the purpose of monitoring, action and follow-up. J. Other	
PF39	With regards to personal information in the service, does the service log the following events: - Creation - Access - Modification - Deletion	1 & 2	A. No – None of the above B. Yes – Some of the above **C. Yes – All of the above (T1, T2)**	NZPP

6.4 Criteria – Interoperability

6.4.1 Interoperability – Data Standards

#	Question	Tier	Notes
DS1	Is the initial provisioning of data into the application aligned with a particular data standard (e.g., SIF AU, SIF NZ, IMS OneRoster)?	1 & 2	Collected for reference only
DS2	Do data export formats from the application align with a particular data standard (e.g., SIF AU, SIF NZ, IMS OneRoster)?	1 & 2	Collected for reference only
DS3	Is all customer data in the service available for export in reusable form?	1 & 2	Collected for reference only A. Yes, self-service at no additional cost B. Yes, at no additional cost C. Yes, at a cost D. No

6.4.2 Interoperability – Technical Integration

#	Question	Tier	Notes
INT1	What standards are supported for **external data integration** with the product (i.e., between a school and the product)? Please list all and version(s) supported.	1 & 2	Collected for reference only

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

INT2	If applicable, what standards are supported for **internal data integration** within the product between various modules or other supporting services? Please list all and version(s) supported.	1 & 2	Collected for reference only
INT3	Have custom APIs been developed for integrating with the product? If so please describe these and provide technical documentation detailing the API (e.g., REST based, JSON payload, etc.)	1 & 2	Collected for reference only
INT4	Has the product undergone any form of standards-based integration assurance testing including Hub Integration Testing Service (HITS) use case integration testing? If so please detail the use cases tested, dates and results (refer: http://www.nsip.edu.au/hits-hub-integration-testing-service)	1 & 2	A. SIF Assurance B. IMS OneRoster conformance certification C. IMS Learning Tools Interoperability (LTI) D. NSIP HITS Testing E. Other (please specify)

6.4.3 Interoperability – Data Availability

#	Question	Tier	Notes
DA1	After exchanging or consuming data into the product how soon is this information available to end users of the product? (e.g., if a new set of school master data is imported via an API, is this available immediately in the product drop downs, reports, etc., is the import manually reviewed and available within 5 business days etc.)?	1 & 2	Collected for reference only

6.5 Evidence

Depending on supplier responses to prior questions, the following documentary evidence is required to be uploaded (system accepts PDF, .DOC, .DOCX).

#	Evidence	Related to question ID
EV1	Attestation of PCI-DSS Compliance	CC2
EV2	ISO27001 Certificate of Compliance / Statement of applicability	CC1
EV3	SOC 2 Type II Certification	CC1
EV4	FEDRAMP (NIST) Certification	CC1
EV5	IRAP Accreditation	CC1

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

EV6	Your organisation's Information Security Policy (external facing)	N/A
EV7	Business Continuity Plan as it relates to the service/s in question	Q2
EV8	Disaster Recovery Plan as it relates to the service/s in question	Q2
EV9	Incident Response Plan or Security Incident Management Plan	T6
EV10	Most recent penetration testing report (redacted) for the service/s in question	T1
EV11	Most recent vulnerability assessment reports (redacted) for the service/s in questions	T1
EV12	Patch management standards / process	T3, T4, T5
EV13	Your organisation's Secure Software Development Lifecycle process	Q5
EV14	Privacy compliance/certification	CC1
EV15	CSA Star	CC1
EV16	HECVAT	CC1
EV17	Sample agreement between service (data integrator, aggregator, data broker, data hub, data distribution hub) and third party	PF33
EV18	A list of all third-party services (company and service names) for which service accounts are required to be created (including access levels e.g., administrator, regular user)	A16A
EV19	Please supply a list of all third-party recipient services (company and service names) including the data types shared (e.g., personal information, medical information, financial data), and the purpose for sharing, with whom the service currently shares data.	PF32

6.6 "Non-compliant" assessment outcome

Questions marked with a hash (#), can lead to a "Non-compliant" assessment outcome if the minimum preferred response/s are not met.

These questions are for Tier 1 products/services: H5, S1, S3, S4, S5, S7, S8, S9, S10, S11, S13, A1, A2, A5, A6, A7, A10, A11, A13, A16b, HR1, HR2, HR3, T1, T2, T3, T6, T7, Q5, D3, D4, CC2, PR1, PR2, PR10, PR12, PR13, PR14, PF6, PF7, PF8, PF9, PF10, PF14, PF18, PF36

For Tier 2 products/services: H5, S1, S3, S4, S5, S7, S8, S10, S11, S13, A1, A2, A13, A16b, T1, T6, T7, Q5, D3, CC2, PR1, PR2, PR10, PR12, PR13, PR14, PF6, PF7, PF8, PF9, PF10, PF14, PF18, PF36

6.7 Updates to the ST4S Criteria, Response Options & Minimum Standards

Given the rapid change to the underlying standards which the ST4S criteria draw on, the ST4S Team is estimating that the ST4S criteria (as represented in this document) will be updated every six months, with release likely occurring in January/February and June/July each year.

6.7.1 Key Changes to the ST4S Criteria (from 2021.2):

The following is a list of the key changes to the ST4S Criteria for 2022.1:

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Current criteria ID	Change	Question/Answer
C0	New	New query to support NZ submissions
C2A/C2B	Change	Change to support capture of AU ABN and NZ NZN
C3A/C3B	Change	Change to support capture of Australian and New Zealand address of organisation
C4A/C4B	Change	Change to support capture of country of registration for AU and NZ customers
C5A/C5B	Change	Change to support capture of preferred contacts for AU and NZ customers
P2B	New	New query re: service free or paid
P2C	New	New URL of service pricing page
P3A/P3B	Change	Change to support capture of AU and NZ URL of service
P6	Change	Included NZ reference
P9	Change	Expanded enrolment support records definition. Added 'Legal status', changed 'unique student identifier' to 'commonwealth unique student identifier (AU) or national student identifier (NZ), updated health and medical details to include mental health diagnoses, added 'use of social services…'
P12	Change	Expanded coverage of requirements for third-party service providers in question definition and updated answer options
H1	Change	Updated question and answer options
H2	Change	Updated question and answer options
H3	Retired	
S1	Change	Updated answer options B, C, D
S2	Change	Updated answer options B, C, D
S3	Change	Updated answer options B, C, D
S7	Change	Updated question text to include 'containers and serverless services'
S9	Change	Updated question text to include 'filtering between network segments'
S10	Change	Updated question text
S11	Change	Updated question text
S13	Change	Updated answer options (removed T1, T2 support for option B)
A2	Change	Updated question text to include support for New Zealand Information Security Manual
A3	Change	Updated question text to include controls limiting predictability
A14	Change	Updated question text to refer to the service itself and not the organisation
A17	New	New question relating to application controls added
HR3	New	New question relating to HR process regarding removal of access to systems

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Current criteria ID	Change	Question/Answer
T1	Change	Added additional response option (external penetration testing)
T3	Change	Updated question text re: patching
T4	Change	Updated question text re: patching
T5	Change	Updated question text re: patching
T7	Change	Updated question text to reference 'affected individuals and what information was disclosed'
Q2	Change	Updated question text to reference 'automated backups and backups that are stored disconnected'
Q6	Change	Updated question text to reference 'a register of all components of the service…'
Q8	New	New question relating to the service's application development added
I1	Change	Updated question text to reference 'security and/or privacy incident or breach'
G04	Change	Updated question and answer options relating to organisation's security and privacy operations teams and real-time monitoring and incident response
PR3A/PR3B / PR3C	Change	Added 'evidence of identity' to all answer options
PR10	Change	Updated question text to support both Australian and New Zealand requirements
PR11	Change	Updated question text and answer options relating to commercial mailing lists
PR12	Change	Updated question text to remove reference specific to Australia
PR13	Change	Updated question text to refer to 'personal information'
PR14	Change	Updated question text regarding discovery functionality to refer to 'personal information'
PF17	Change	Added response option E – Not applicable.
PF34	Change	Retired
PF38	Change	Updated question text (minor)
PF39	New	New question added regarding logging of creation/access/modification / deletion of personal information
PF40-PF50	New	New questions added covering additional integrator/data hub/data aggregator functionality
DS1, DS2	Change	Updated question text to include NZ specific examples
DS3	New	New questions added regarding export of customer data
INT4	Change	Updated question and answer options relating to standards-based integration testing

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Current criteria ID	Change	Question/Answer
EV19	Change	Updated evidence text requesting detail on ‘data types shared and purpose for sharing’
All	Change	Updated Australian ISM references to include AU prefix. Added NZ ISM references (NZ prefix)

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Appendix A – Tier Self-Assessment

The breadth and depth of an assessment performed on a supplier's service is based on the assessment tier. Three factors contribute to a service's tier categorisation:

1. Data: The data stored or processed by the service.
2. Functionality: The service's functions.
3. Reasonableness: The service's display and communication of advertising or other materials which may cause offence.

The tier used for assessment purposes is the highest tier that the service qualifies against across all three categories.

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

Tier Self-Assessment

	Tier 1	Tier 2	Tier 3
Data	Sensitive information Financial information Health information Government Identifiers	Personally identifiable information (PII)	Non-PII Public domain information
Functionality	Remote access Learning management systems School administration Systems Financial management systems Behavior management Systems Teacher professional development tools File storage Customisable functionality Video or student diary or communication tools. Video capture/audio/ webcam functions Services with multiple primary purposes/ functionalities	Chat/Instant or delayed messaging Blogs Email Message boards File sharing Screen sharing Social media account sharing/integration Photo posting/sharing Contain, display or promote: Political material Market places for the exchanges of goods/ services	
Reasonableness	Advertising of products/ services in the following categories: alcohol, controlled or banned substances, gambling, tobacco products, firearms and fire arm clubs, adult products and pornography. Any function or display of information which may be deemed offensive by a reasonable member of the school community (e.g., racist, sexist content).	Contain, display or promote: Sensitive topics which may cause offense in the community	

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

1) Data		
Assessment Tier	Data Definitions	Data examples
Tier 1	Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. It also includes health information and biometric information. Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service. Financial information covers individual, family, staff, student financial records, bank details, debts, debt reminders etc. Identifiers covers government or other allocated identifiers which are possibly sensitive for the purposes of tracking an individual.	Sensitive information, including: for students: religion, birth certificate, language spoken at home, religious records (for example Baptism Certificate), religious education, whether Aboriginal or Torres Strait Islander, nationality, country of birth, legal information (custody, legal orders, out of home care), geographic location (GPS/lat/long), biometric data (eye/retinal imagery, fingerprints), welfare and discipline reports, passport details for parents: place of birth, religions, religious education, criminal record check, relevant child protection information (including working with children checks if volunteering to assist in the classroom), country of birth, whether Aboriginal or Torres Strait Islander, and nationality, legal information (custody, legal orders, out of home care), marital status/problems, voting in board elections for job applicants, staff and contractors: place of birth, religion, religious education, criminal record check, relevant child protection information (including working with children checks), member of professional associations, trade union membership, country of birth, nationality, OHS incident reports, staff complaints, workplace issue reports, letters of appointment/ complaint/ warning/ resignation, professional development appraisals, performance review, passport details Health information, including: • for students: medical background, immunisation records, medical records, medical treatments, accident reports, absentee notes; medical certificates, health and weight, nutrition and dietary requirements, assessment results for vision, hearing and speech, reports of physical disabilities, illnesses, operations, paediatric medical, psychological, psychiatric, learning details (recipient special procedures), assessment for speech, occupational, hearing, sight, ADD, Educational Cognitive (IQ), health or other gov. service referrals • for parents: history of genetic and familial disorders (including learning disabilities), miscellaneous sensitive information contained in a doctor or health report; and

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

1) Data		
Assessment Tier	Data Definitions	Data examples
		• for job applicants, staff members and contractors: medical condition affecting ability to perform work, health information, medical certificates and compensation claims. Financial information including: Credit card details, account details, payment overdue notices, financial information relating to payment of school and administrative fees, banking details, scholarship details and information about outstanding fees, donation history, details of previous salary, salary being sought and other salary details, superannuation details Identifiers includes: local, state and federally or nationally assigned student, parent or staff identifiers (government related identifiers) Examples: Tax File Number, Victorian Student Number, Medicare number, Drivers License number, Passport, teacher registration number.
Tier 2	Personal information not captured in the 'High' tier: Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source. In other words, if the information or opinion identifies an individual or allows an individual to be identified it will be 'personal information' within the meaning of the Privacy Act. It can range from very detailed information, such as medical records, to other less obvious types of identifying information, such as an email address. Personal information does not include information that has been de-identified so that the individual is no longer identifiable	for students: name, sex/gender, physical address, email address, social media handles, phone number, date of birth (and age), conduct reports, next of kin details, emergency contact numbers, names of doctors, school reports and exam/test results, attendances, assessments, previous school history, referrals (e.g. government welfare agencies/departments), correspondence with parents, photos, current/previous school, health fund details for parents: name, physical address, email address, phone number, date of birth, vehicle registration details, occupation, doctor's name and contact information, other children's details, maiden name of ex-pupils, alumni year, whether alumni had further education, professional experience and personal news for job applicants, staff and contractors: name, company name and ABN, phone number, physical address, email address, date of birth and age, contact details of next of kin, emergency contact numbers, including doctor, residency status/work visa status, qualifications, education, academic transcript, work

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

1) Data		
Assessment Tier	Data Definitions	Data examples
		permit, details of referees, marital status, record of interview, leave applications, photograph, applications for promotions, references, commencement date, employment agency details, former employers.
Tier 3	Non-PII data. Data not falling into either the High or Medium sensitivity tiers. Data in this tier is typically in the public domain or presumed to pose low or no risk.	Data assumed to be in public domain or low / no risk data

2) Functionality / Purpose of service & 3) Reasonableness		
Tier	Functionality	Reasonableness
Tier 1	Products which offer generic functionality in any of the following categories will be deemed as falling into tier 1: o Remote access Products in the following broad product categories will be deemed as tier 1: o Learning Management/ Student management and learning support systems e.g., student work, assessment, academic results, timetabling, pastoral care, communication; o School administration systems, including student records, attendance, data collection e.g., enrolment, consent management; o Financial management/ payment collection systems; o Behaviour management systems; o Teacher professional development tools/record keeping systems; o File storage e.g., iCloud, Dropbox, Google Drive; o Services with customisable functionality - site specific (including integration with enterprise solutions or additional third-party services); o Video or student diary or communication tools (parent, teacher, child); o Video capture/audio/webcam functions;	Products which may contain, display or promote the following categories of information will be deemed as falling into tier 1: o Advertising of products/services in the following categories: alcohol, controlled or banned substances, gambling, tobacco products, firearms and fire arm clubs, adult products and pornography. o Any function or display of information which may be deemed offensive by a reasonable member of the school community (eg racist, sexist content)

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.

	o Services with multiple primary purposes/functionalities (e.g., combination of those listed in Tier 2)	
Tier 2	Products which offer functionality in any of the following categories will be deemed as falling into tier 2: o Chat/Instant or delayed messaging o Blogs o Email o Message boards o Screen sharing o Group calls o File sharing o Photo posting/sharing o Social media account sharing/integration (e.g., Facebook, Google) o Market places for the exchanges of goods/services	Products which may contain, display or promote the following categories of information will be deemed as falling into tier 2: o Political material o Sensitive topics which may cause offense in the community
Tier 3	N/A	N/A

Unless otherwise indicated, the copyright in this Vendor Guide is owned by Education Services Australia Ltd and is subject to the Copyright Act 1968 (Cth). You must NOT reproduce, publish, perform, communicate, distribute or transmit all or part of this Vendor Guide without the prior written permission of Education Services Australia Ltd.