Safer Technologies for Schools Assessment:

Vendor Guide

Guide for vendors participating in the Safer Technologies for Schools Assessment process (ST4S) (previously known as the National Education Risk Assessment).

Release:	2021.1
Date of this version:	23-Jun-21
Author:	ST4S Team
Document Version Number:	1.2 Final
Location:	Latest version available www.st4s.edu.au

Important information including disclaimer:

This guide is provided:

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

Education Services Australia Limited through its business unit the National School's 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 States and Territories 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 States and Territories 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).

Contents

Version Control & Latest Version

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

Version Control			
Version	Date:	Author/Organization:	Comments
V0.1	9/02/2021	ST4S Team	Initial draft
V0.4	26/02/2021	ST4S Team	Final draft
V1.0	1/3/2021	ST4S Team	Document made final
V1.1	17/5/2021	ST4S Team	Copyright statement updated
V1.2	23/6/2021	ST4S Teams	Updated references to non-compliant items. Included references to ST4S website (www.st4s.edu.au)

1. Introduction

1.1 Purpose

This vendor 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
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 VWG	Safer Technologies for Schools Vendor Working Group
NSIP	National Schools Interoperability Program (www.nsip.edu.au), a business unit of ESA

1.3 Background

- Schools and school authorities have obligations stemming from Federal and State legislation to protect the privacy and security of 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.
- 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.
- 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 ST4SWG have developed a common evaluation process and assessment criteria covering the key domains of trust namely: security, privacy, interoperability and online safety.

- As vendors 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 eSafety Commissioner's Safety by Design (SbD) initiative 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. Vendors are encouraged to become familiar with the SbD principles. Tools and resources to support vendors to embed user safety into the design of their products or services will be made available on the eSafety website throughout 2020.

1.4 Benefits of a national approach

- Most State and Territory agencies have established local risk assessment teams or are planning to do so.
- The anticipated benefits of a national 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 vendors to demonstrate compliance with national security, privacy and interoperability standards.
    - An incentive for vendors to comply with security, privacy and interoperability standards.

1.5 Vendors not in scope for assessment

Not all vendors are in scope for participation in the assessment process. The ST4S Working Group, in consultation with the NSIP Steering Group, is responsible for determining the assessment priority of vendor products and services. Vendors offering additional services or vendors not in scope for the assessment will not be able to participate at this stage but can use these guidelines to help direct compliance efforts.

2. Assessment process

2.1 Generation of School Level Reports

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

2.2 Release of findings to vendors

Vendors will receive a draft of the school level report which is generated based on the responses provided to the vendor questionnaire. Vendors may also receive a spreadsheet containing questions on which the assessment team is seeking further clarification. Vendors are asked to respond to the clarifications within the timelines as directed. Vendor 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, vendors 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 vendor's nominated contact. The exception to this release timeline is where a vendor has received a non-compliant outcome. Vendors will be notified if this is the case and informed of applicable timeframes.

2.3 Findings outcomes

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 vendor's product or service results in one of the following outcomes:

Use Responsibly *Use with Caution*

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 vendor 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.

2.5 Challenging findings

As part of the development of the final school level reports, vendors 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 vendor as the outcomes are dictated by the guidance in the ST4S Vendor Guide. If a vendor considers a school level report is not accurate, that vendor may lodge a request to have their report re-reviewed. In order to request a re-review, vendors need to provide relevant details to the contact point detailed in Section 4 below.

2.6 Re-assessment

Subject to resourcing and prioritisation, vendors 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 vendor product/service and/or occurrence of a breach or security incident.

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 reports

3.1 Findings distribution across States, Territories, Catholic and Independent Sectors

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 jurisdiction authority.

3.2 Sharing of findings with Trusted Parties

When responding to the questionnaire vendors 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 vendor.

3.3 Sharing of findings with Vendors

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

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

3.4 Vendor use of the findings internally

One of the goals of the ST4S process is to influence vendors 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. Vendors can continue to improve their products/services over time and are encouraged to continue to reference the ST4S standards (as documented in the ST4S Vendor Guide) as it is updated over time.

3.5 Guidance regarding Vendor use of assessment outcomes

Vendors 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. Vendors must not provide the ST4S assessment report or any copies or extracts of it to anyone outside the vendor organisation (for example, schools or school communities).
3. Vendors 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. Vendors must acknowledge and communicate with customers that an ST4S assessment outcome does not necessarily mean that the vendor is compliant with local State/Territory or Non-Government sector requirements.
5. Vendors must direct enquiries from schools regarding the provision of detailed reports to the relevant education authority (Government schools to the relevant State/Territory Department of Education, Catholic schools to their

local State or Diocese office and Independent schools to their State/Territory association) as listed on the final report.

6. Vendors must not edit or modify their final or draft school-level reports in any way.
7. Vendors must not claim that a ST4S assessment applies to other products, services, or modules offered by the vendor, or different versions of the product, service or module.
8. Vendors 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. Vendors 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. Vendors must not publish in whole or in part the ST4S assessment results for another vendor's service.
11. Vendors must notify the ST4S Assessment Team if they come into possession of some or all of another vendor's ST4S report or results.
12. If a vendor does not comply with the above usage conditions, the ST4S Assessment Team may rescind/withdraw/modify that vendor'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.

Vendors should direct 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

Vendors should direct non-government schools queries to the relevant authority listed below:

- Catholic and Independent Schools
  - Catholic Education – Contact the relevant local jurisdiction ie diocese, CEnet or commission.
  - Independent schools – Contact the local AIS operating in your State or Territory.

Requirements for Non-compliant and Non-participating vendors:

1. If approached by current or potential customers regarding the ST4S process, vendors 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 Vendor Guide:

1. This Vendor 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 Vendor Guide is accurate and up-to-date, the Vendor 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 Vendor Guide; and
    - is not liable for any loss or damage however caused resulting from the use or inability to use the Vendor Guide or caused to any property as a result of the use of the Vendor 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.

- 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.
- 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.
- Participating stakeholders outside of the ST4S assessment team may seek further detail from vendors 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 vendor's sole risk, cost and expense. NSIP will not be responsible for any costs or expenses incurred by a vendor 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 vendor and NSIP, the assessment service or any stakeholders in ST4S.
- NSIP is not liable to any vendor 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 vendor'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 State and Federal Government information security classification frameworks. Vendor responses will assist in the assessment, mitigation and monitoring of the risks associated with their product/service.
- 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.

5.2 Completion of the Questionnaire

- Vendors 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.
- All questions are mandatory, and vendors will not be able to navigate between pages without first completing the questions on the page displayed.
- If at any time vendors are not sure which product, module or component is the subject of the response, please contact the assessment team.
- If the vendor'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 vendors 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).
- Vendors will be able to partially complete the questionnaire and return at a later time to complete it.
- Vendors may choose to download a copy of their responses to the questionnaire prior to submitting.
- Vendors 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, vendors 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;
    - 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 vendors.

6 Assessment Criteria

6.1 Criteria – Company & product detail

#	Question	Tier	Notes
C1	Vendor name	1 & 2	Informational
C2	Vendor ABN	1 & 2	Informational
C3	Registered address of vendor	1 & 2	Informational
C4	Country in which the company is registered	1 & 2	Informational
C5	Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	1 & 2	Informational

6.2 Criteria – Security

Standard references are taken from:

- the Australian Government Information Security Manual (ISM): https://www.cyber.gov.au/ism; and
- the Australian Privacy Principles (APP): https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/.

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 and
- an asterisk * 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		
P2	Version of service *If no published version number, use date of version.*	All		
P3	URL of service for Australian customers	All		
P4	URL of Terms of Service/use	All		
P5	In 50 words or less describe the purpose of the service?	All		
P6	In what jurisdiction would disputes of any kind, regarding usage of the service, be handled? (e.g., Victoria Australia)	1 & 2		

P7	Does your organisation have a current insurance policy of at least $1m with claims for data breach/loss?	1	**A. Yes - current policy with coverage of at least $1 million (T1)** B. Yes - current policy but coverage is less than $1 million C. No current policy	
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	
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*	All	A. Sensitive personal information and records about individuals (including students, parents, staff, job applicants and contractors) B. Health and medical information C. Financial information D. Government related Identifiers (e.g., state or federal government assigned identifiers) E. Records, certificates, and documents (e.g., government issued identification documents, passport, birth certificate, driver licence, complaints, performance reviews) F. Racial or ethnic origin (e.g., languages, nationality, country of birth, indigenous status) G. Religious beliefs or affiliations H. Sexual orientation or practices I. Biometric information (e.g., eye/retinal imagery, fingerprints, biometric templates) **J. None of the above (T2)**	

	- Student support service information and support arrangements *- Enrolment support records (sensitive case, complex case, adjustments, student plan, developmental map, transportation)*			
P10	Select the functionality available within the service. Select all that apply.	All	A. Learning management and learning support systems B. School and student administration systems, including student records, attendance, data collection e.g. enrolment, consent management C. Financial management and/or payment collection systems D. Behaviour management systems E. Teacher professional development tools/record keeping systems F. Cloud file storage G. Video or student diary or communication tools (parent, teacher, child) H. Services with customisable functionality - site specific (including integration with enterprise solutions or additional third party services) **I. None of the above (T2)**	
P11	Does the service contain, display, or promote the following categories of information: • 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, pornographic content etc.)	All	A. Yes (please specify) **B. No (T2)**	
P12	Does your organisation have contractual agreements in place to ensure any third party providers that make up the solution, or provide service to you, adhere to your information security and privacy policies?	1	A. No B. Yes - with some third parties **C. Yes - with all third parties (T1)** **D. NA - solution does not use third party providers (T1)**	

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)**	

6.2.2 Security – Hosting and Location

Q	Question	Tier	Response options	Standard
H1	Select the option which best describes how all components of the service, including live solution, backup, disaster recovery, test environment, and development environment are hosted.	1 & 2	A. Hosted entirely onshore in Australia (T1, T2) B. Hosted entirely offshore outside of Australia (specify countries) C. Partially hosted offshore outside of Australia – live solution offshore, remaining components hosted onshore (specify countries). D. Partially hosted offshore outside of Australia – live solution onshore, remaining components hosted offshore (specify countries).	ISM Security Control: 1452 Revision 3
H2	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) from any country other than Australia?	1 & 2	**A. No (T1, T2)** B. Yes (specify countries)	ISM Security Control: 0975 Revision 7
H3	Is user data and any related data (e.g. metadata, logs) held by the service ever taken, sent or transmitted outside of Australia for storage, maintenance or any other purpose? If yes provide details.	1 & 2	**A. No (T1, T2)** B. Yes (specify countries & purpose)	ISM Security Control: 1572 Revision 0

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	ISM Security Control: 1296
H5#	Are customers notified of migration of the cloud infrastructure, including system components, user data and related data, and vendor staff, to offshore locations outside of Australia prior to implementation?	1 & 2	A. No **B. Yes (specify average notification lead time) (T1, T2)**	ISM Security Control: 1578 Revision 0
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 (T1, T2)** **D. Not applicable – service does not include outsourced cloud-based services (T1, T2)**	ISM 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 B. Encryption: DES, RC4; 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, 3DES using three distinct keys; Hashing: SHA-224 or above;	ISM Security Control: 1139, revision 5; ISM Security Control: 0471, revision 6; ISM Security Control: 1277, revision 2.

			Digital Signatures: DSA (2048), ECDSA (224) or RSA (2048); Key Exchange: DH (2048), ECDH (224), RSA (2048); Protocol: TLS1.2 or above only. (T2) D. Encryption: AES 128 or above only (AES 256 recommended) Hashing: SHA-256 or above only (SHA-384 recommended) Digital Signatures: DSA (2048+) ECDSA (256) or RSA (2048+); Key Exchange: DH (3072+), ECDH (P-256) and/or RSA (2048+) Protocol: TLS1.2 or above only (TLS 1.3 recommended). (T1)	
S2	What are the minimum encryption algorithms applied to protect data at rest, including backup, storage and audit logs?	1 & 2	A. No encryption B. DES, RC4 **C. AES 128, 3DES using three distinct keys (T2)** **D. AES 192, AES 256 (T1)** E. Encryption algorithm equivalent to options C or D (please specify equivalent algorithms)	ISM Security Control: 0459, revision 3
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 B. Encryption: DES, RC4; 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, 3DES using three distinct keys;** **Hashing: SHA-224, SHA-256, SHA-384, and SHA-512;**	ISM Security Control: 1139, revision 5; ISM Security Control: 0471, revision 6.

			Digital Signatures: DSA (1024+), ECDSA (160+) or RSA (1024+); **Key Exchange: DH (1024+), ECDH (160+) and/or RSA (1024+);** **Protocol: TLS 1.2 or above only(T2)** **D. Encryption: AES 128 or above only (AES 256 recommended);** **Hashing: SHA-256 or above only (SHA-384 recommended);** **Digital Signatures: DSA (2048+) ECDSA (256) or RSA (2048+);** **Key Exchange: DH (2048+), ECDH (P-256) and/or RSA (2048);** **Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)** E. N/A - Customer data is not uploaded to the service	
S4#	Is data segregation used to isolate one customer's data from another customer's data? e.g., Logical segregation at the user access level, separate storage and database instances per customer, physical segregation (separate infrastructure) for each customer, virtual segregation (separate cloud infrastructure tenancies or virtual private clouds) for each customer.	1 & 2	A. No **B. Yes (T1, T2)**	ISM Security Control: 1436, revision 1
S5#	Are all of the service's web servers secured with digital certificates signed by a trusted authority?	1 & 2	**A. Yes (please specify CA) (T1, T2)** B. No	ISM Security Control: 1161
S6	Does your organisation have a documented and implemented key management process which describes at a minimum: • Key generation; • Key registration; • Key storage; • Key distribution and installation;	1	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1)**	

	• 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) 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 B. Yes - some of the above **C. Yes – all of the above except HIPS (T2)** **C. Yes - all of the above (T1)**	ISM Security Controls: 1341, 1034, 1416, 1417
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 B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	ISM Security Controls: 1246, 1247, 1249, 1250, 1260, 1262, 1263, 1273
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) • DMZ for internet-facing components and separate trusted zones for other components • Virtual (e.g. VLAN) or physical network segregation	1 & 2	A. No – none of the above B. Partial – secure communication or DMZ C. Partial – virtual or physical network segregation (T2) **D. Yes – all of the above (T1, T2)**	ISM Security Control: 1436, revision 1
S10#	Does your organisation have a documented and implemented system hardening process which:	1 & 2	A. No - none of the above B. Yes - some of the above	Security Control: 1406 Revision: 2; Security Control:

	• Includes in scope operating systems, virtualization platforms, storage, network and applications; • Ensures only required ports, protocols, services and authorisations are enabled (all others are restricted); and • Is reviewed annually.		C. Yes – all of the above except annual review (T2) **D. Yes - all of the above (T1)**	1585 Revision: 0; Security Control: 1605 Revision: 0; Security Control: 1588 Revision: 0.
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; • DoS/DDoS (Denial of Service/Distributed Denial of Service) defence; and • Web Application Firewall (WAF)?	1 & 2	A. No - none of the above 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)**	Security Control: 1528 Revision: 1; Security Control: 1435; Revision: 1.
S12	Has your organisation developed and implemented a security policy governing the management of mobile devices, and does the organisation use a Mobile Device Management solution to ensure the mobile devices management policy is applied to all mobile devices?	1 & 2	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1)**	
S13#	Is production data used in non-production (e.g., test and development) environments?	1 & 2	A. No (T1, T2) **B. Yes - with identical security controls applied and/or with production data obfuscated/de-identified (T1, T2)** C. Yes – without identical security controls applied and obfuscation or de-identification of production data.	Security Control: 1420 Revision: 2.

6.2.4 Security – Logging

Q	Question	Tier	Response options	Standard
L1	Do all systems in your organisation (e.g., servers, storage, network, applications, etc.) log the following: • Successful log ins; • Unsuccessful logins; • Date and time of each event; • Log offs; • Unauthorized access attempts; • User administration (e.g., adding, modifying, deleting users); • Password changes; • Security configuration changes; • System events (restarts and shutdowns); • Access to log files; • Privileged access activities; • Security related system alerts and failures; and • Synchronised to an accurate time source?	1 & 2	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	ISM Security Controls: 0584, 0585, 0582, 1536, 1537
L2	Does your organisation have a proactive 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)**	ISM Security Control: 0109
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)**	ISM Security Control: 1405

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 **B. Yes (T1, T2)**	ISM Security Control: 0414

A2#	Are all passwords used to access the service (i.e. user, system, and privileged account passwords) protected in line with the recommendations in the Australia Cyber Security Centre 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 **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)**	ISM Security Control: 1252
A3	At a minimum, are the following password requirements enforced for vendor staff access to the organisation's systems and the service: • if using single factor authentication, passwords/passphrases are a minimum of 14 characters with complexity • if using multi-factor authentication, passwords are a minimum of six characters	1 & 2	A. No **B. Yes (T1, T2)**	ISM Security Control: 0421
A4	Within the service, do you offer two-factor authentication for end-users?	1	A. No **B. Yes, offered as an option (T1)** **C. Yes, mandated for end users (T1)**	ISM Security Control: 0974
A5#	Does your organisation **mandate** two factor authentication for: • Vendor staff accessing systems remotely; • System administrators; • Support staff; and • Staff with privileged accounts?	1 & 2	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	ISM Security Control: 1173 Revision 3
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 B. Yes, for some systems **C. Yes, for all systems (T1,T2)**	
A7#	At a minimum, is vendor staff 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 **B. Yes (T1, T2)**	ISM Security Controls: 0405, 0430, 1404

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 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)**	ISM Security Control: 1503
A10#	Are all internal organisation systems configured with a session or screen lock that: • 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?	1 & 2	A. No B. Yes, some of the above **C. Yes, all of the above (T1, T2)**	ISM Security Control: 0428
A11#	When a password reset is requested by the user but performed by the service, 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 B. Yes, some of the above **C. Yes, all of the above (T1, T2)**	ISM Security Controls: 1227, 1593, 1594, 1595
A12	Does the service allow user registration or logon/authentication via credentials provided by another Identity Provider (IDP) such as RealMe, Facebook, Google, Microsoft etc.	1 & 2	A. No B. Yes, please specify.	

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 default (Deny unless approved) (T1, T2)** B. Protection by exception (Allow access unless specifically denied)	

6.2.6 Security – HR

Q	Question	Tier	Response options	Standard
HR1#	Do all vendor staff 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 **B. Yes (T1, T2)**	ISM Security Control: 0434
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; 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?	1 & 2	A. No - none of the above B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	ISM Security Control: 0252

6.2.7 Security – Processes and Testing

Q	Question	Tier	Response options	Standard
T1#	Does your organisation have an implemented continuous monitoring plan 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 B. Yes - meets some of the requirements above **C. Yes - meets all requirements above (T1, T2)**	ISM Security Control: 1163
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 B. Yes - some of the above **C. Yes - all of the above (T1, T2)**	ISM Security Controls: 0298 revision 7, 0303, 1499, 1497, 1500.
T3#	Are security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as **extreme risk** patched or mitigated within **48 hours** of being identified?	1	A. No **B. Yes (T1)**	ISM Security Controls: 1144, 1494
T4	Are security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as **high risk** patched or mitigated within **two weeks** of being identified?	1 & 2	A. No **B. Yes (T1, T2)**	ISM Security Control: 0940, 1495
T5	Are security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as **moderate or low risk** patched or mitigated within **one month** of being identified?	1 & 2	A. No **B. Yes (T1, T2)**	ISM Security Controls: 1472, 1496
T6#	Does your organisation have a formal and documented incident response plan which requires security, privacy and online safety incidents to be:	1 & 2	A. No - none of the above **B. Yes - some of the above (T2)** **C. Yes - all of the above (T1)**	ISM Security Control: 0125

	• Investigated; • Remediated; and • 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?	1 & 2	A. No - none of the above **B. Yes - notification of breach only (T2)** **C. Yes - all of the above (T1, T2)**	ISM Security Controls: 0123, 0141, 0140
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 - notification of loss or corruption only (T2)** **C. Yes - notification of loss or corruption which includes details (T1, T2)**	ISM Security Controls: 0123, 0141, 0140

6.2.8 Security – Plans and Quality

Q	Question	Tier	Response options	Standard
Q1	Are system and platform changes and upgrades that cause service disruption completed outside of core business hours?	1	A. No **B. Yes (T1)**	
Q2	Does your organisation have a documented and implemented Business Continuity Plan for the service which includes: • Backup strategies; • Restoration strategies (e.g. disaster recovery); and • Preservation strategies?	1	A. No B. Yes - meets some requirements **C. Yes - meets all requirements (T1)**	ISM Security Controls: 1547, 1548, 1510
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 • Categorisation of IT change (e.g., Standard, Pre-Approved, Emergency, etc.);	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)**	ISM Security Control: 1211

	• 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)**	ISM Security Control: 1636, revision 0, ISM Security Control: 1526, revision 1
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	1 & 2	A. No B. Yes - security testing partially satisfies the guidance provided in an industry standard framework (please specify framework)	ISM Security Control: 1239

	(OWASP) Testing Guide v4.2, Building Security In Maturity Model (BSIMM))?		**C. Yes - security testing fully satisfies the guidance provided in an industry standard framework (T1, T2) (please specify framework)**	
Q6	Does your organisation have a documented and implemented IT Asset management process including: • 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)**	ISM Security Control: 0336, revision 4, ISM Security Control: 0159, revision 4
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)**	ISM Security Control: 1478 revision 1.

6.2.9 Security – Incidents

Q	Question	Tier	Response options	Standard
I1	Has the organisation, platform, or service had a recent security 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)**	ISM Security Control: 1514

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)**	
D3#	Is the full restoration of backups tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur (e.g., technology stack changes, vendor changes, platform changes)?	1 & 2	A. No **B. Yes (T1, T2)**	ISM Security Control: 1515
D4#	Is the partial restoration of backups tested on a quarterly or more frequent basis?	1 & 2	A. No **B. Yes (T1, T2)**	ISM Security Control: 1516

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 any third party services it relies on (e.g. cloud providers, third party developers).	1 & 2	A. IS27001 B. SOC 2 Type II C. FEDRAMP (NIST) D. IRAP E. Privacy confirmation (GDPR, SOPAA, Privacy Shield etc.) F. CSA STAR G. HECVAT H. Other I. None of the above	
CC2#	If the solution processes electronic payments or holds credit card data is it Payment Card Industry (PCI) Data Security Standards (DSS) compliant?	1 & 2	A. No **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)**	

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)**	

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).**	
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)**	

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; and • Required to be agreed to by the customer prior to account registration (e.g., via checkbox, etc.)?	1 & 2	A. No B. Yes - some of the above **C. Yes - all of the above (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 **E. NA - this service will not be used by students (T1, T2)**	
PA3	What are the specified definitions of intellectual property ownership in the terms of use for the service? (i.e., work created within and/or uploaded to the service)? 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. **C. 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 **B. Yes - some of the above (T1, T2)** **C. Yes - all of the above (T1, T2)**	APP: 1.5
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 • 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?	1 & 2	A. No B. Yes - includes some of the above **C. Yes - includes all of the above (T1, T2)**	APP: 1.4
PR3	What **mandatory** information is collected by the service during the **standard account registration process**? Select all that apply. If not required select N/A *'Standard' account creation refers to individual users creating their own accounts. If your service offers a 'for home use' and a 'for school use' version, please answer based on what is required for **school use only**.*	1 & 2	Information, used to inform consent requirements. However, services should only collect information that is necessary to perform the intended function e.g., It is, for example, difficult to see why "sex/gender" would be necessary to collect in many circumstances, or even last name in some circumstances. A. First name (please specify if student, school staff, or parent)	

			B. Surname (please specify if student, school staff, or parent) C. Email address (please specify if student, school staff, or parent) D. Gender (please specify if student, school staff, or parent) E. Date of birth (i.e., dd/mm/yy) (please specify if student, school staff, or parent) F. Age, month and year of birth, or year of birth (please specify if student, school staff, or parent) G. Year level K. Country or state/province (please specify if student, school staff, or parent) L. Evidence of identity	
PR3A	Is any other mandatory information collected during the standard account registration process?	1 & 2	A. Yes (please specify) B. No (T1, T2) C. N/A - accounts are not required to use this service (T1, T2)	
PR4	If the school, teacher, or the service generates accounts for school staff, student, or parent use, what mandatory information is collected by the service? Select all that apply. If not required, select N/A. *This question refers to when a school teacher is registering accounts on behalf of others (e.g., students, other staff, or parents). If your service offers a 'for home use' and a 'for school use' version, please answer based on what is required for* ***school use only****.*	1 & 2	Information, used to inform consent requirements. However, services should only collect information that is necessary to perform the intended function e.g., It is, for example, difficult to see why “sex/gender” would be necessary to collect in many circumstances, or even last name in some circumstances. A. First name (please specify if student, school staff, or parent) B. Surname (please specify if student, school staff, or parent) C. Email address (please specify if student, school staff, or parent) D. Gender (please specify if student, school staff, or parent)	

			E. Date of birth (i.e., dd/mm/yy) (please specify if student, school staff, or parent) F. Age, month and year of birth, or year of birth (please specify if student, school staff, or parent) G. Year level K. Country or state/province (please specify if student, school staff, or parent) L. Evidence of identity	
PR4a	Is any other mandatory information collected when the school, teacher, or service generates accounts for schools, staff, student or parent use?	1 & 2	A. Yes (please specify) **B. No (T1, T2)** **C. N/A - accounts are not required to use this service (T1, T2)**	
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., use of pseudonym or de-identified information)? Please include excerpt from the terms of service.	1 & 2	A. Yes (please include excerpt from the terms of service) **B. No (T1, T2)**	
PR6	Are customers/users offered anonymity and/or pseudonymity when dealing with the service provider in some circumstances (e.g., logging support requests, providing feedback)?	1 & 2	A. No **B. Yes, please specify circumstances (T1, T2)**	APP: 2.1
PR7	Are mandatory fields clearly distinguished from optional fields during the standard account registration process?	1 & 2	A. No **B. Yes (T1, T2)**	
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)**	
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)**	
PR10#	Does your organisation share user data with third parties in any circumstance other than the following? If yes, please specify.	1 & 2	A. Yes (please specify) **B. No (T1, T2)**	APP: 6.1, 6.2

	-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 an Australian law or a court/tribunal order; -a permitted general situation exists in relation to the use or disclosure of the information (www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-c-permitted-general-situations/); -a permitted health situation exists in relation to the use or disclosure of the information (www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-d-permitted-health-situations/); and -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?			
PR11	Is subscription to the service's mailing list opt-in by default? *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 of the service's mailing list **B. No - opt-out by default** **C. Yes (T1, T2)** **D. N/A - no mailing list (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 an Australian law or a court/tribunal order;	1 & 2	A. Yes (provide details of the identifier(s) and how each is used) **B. No (T1, T2)**	APP: 9.1, 9.2

	• 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; • User or disclosure is necessary for the organisation to fulfil its obligations to an agency or State or Territory authority; • Use or disclosure is required or authorised by or under an Australian law or court/tribunal order; • 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 users or organisations (in the case of enterprise offerings) to request the service to provide, modify, **and** delete all personally identifiable information relating to them?	1 & 2	A. No 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 personally identifiable information	APP: 12.1, 13.1
PR14#	Does the service provide any discovery functionality which allows users from one school to find, access or discover users 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 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	

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 (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. 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 and/or games O. Administrative support services and records management P. Other Q. 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. Surveys - service provider generated, non-editable C. Online forms - customisable / user generated D. Surveys - customisable / user generated E. eSignatures (please specify mechanism) 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	

			H. Participants are not notified if they are participating in a recorded session (e.g., via on screen prompt)	
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 are initiated and/or accepted by the user handing over control C. Onscreen notification is displayed throughout remote access sessions D. Remote access sessions are not logged	
PF8	In relation to the screen sharing functionality available within the service, select all that apply.		A. Screen sharing can be disabled by an administrator or moderator B. Screen sharing sessions are initiated and/or accepted by the user who is sharing their screen C. Screen sharing sessions are not logged	
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-members (i.e., no log in is required to participate in chat/messaging) F. Chat can be restricted to between members of the service only (i.e., only account holders can communicate with each other) G. An administrator/teacher can control who users can chat with/message (i.e., a teacher can restrict students to only chat/message with classmates) H. Chat/instant messaging can be disabled by an administrator/moderator	

			I. Chat/instant messaging is visible to an administrator (e.g., teacher) in real time J. Chat/instant messaging is not logged K. Other L. None of the above	
PF10	In relation to the commenting 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) 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 are inappropriate or that breach the service's guidelines D. Users can report comments that are inappropriate or that breach the service's guidelines E. Comments are reviewed by an administrator or the service prior to publishing F. Commenting can be disabled by an administrator/moderator G. An administrator/teacher 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 J. Users can upload and/or share projects or files in forums/communities K. Other L. 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	
PF12	In relation to the quiz, poll and flashcard creation and distribution functionality available within the service, select all that apply.		A. Quizzes, polls and/or flashcards can be distributed and/or shared via linked social media accounts (Facebook, Twitter etc.) B. Quizzes, polls and/or flashcards can be shared as templates for re-use by others. C. None of the above	
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: • Files are scanned for Malware/Viruses during download; • Files are scanned for Malware/Viruses while at rest; and • Files found to contain Malware/Viruses are deleted or quarantined?		A. None of the above 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)**	ISM Security control: 0657
PF15	When sending user initiated correspondence, how does the service send email communication? Select all that apply.		A. Displaying the user provided email address as the sender B. Displaying the user@theservicename as the sender C. Through unverified email addresses which may be anonymous or invalid (and can't be tracked or audited) 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 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. Files can be shared via linked social media accounts (Facebook, Twitter etc.) B. Authors have control over who can view and/or edit their files C. Administrators (e.g., teachers) can restrict who can view and/or edit users' files D. Administrators can disable file sharing E. None of the above	
PF18	At a minimum, are the following features built into the file upload functionality available within the service? • Files are scanned for Malware/Viruses during upload • Files are scanned for Malware/Viruses while at rest • Files found to contain Malware/Viruses are quarantined or deleted		A. None of the above B. Yes, some of the above C. Yes, all of the above (T1, T2)	ISM Security control: 0657
PF19	In relation to the content creation functionality available within the service, select all that apply.		A. Account holders can share the content they have created (e.g., via direct urls) B. Account holders can share the content they have created via linked social media accounts C. Authors have control over who can view and/or edit the content they have created D. Administrators (e.g., teachers) can restrict who can view and/or edit users' content	

			E. Administrators can disable sharing of users' content F. Account holders are not notified if their content is on-shared G. 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 is published to the service by default and publication cannot be disabled B. User generated content is published to the service by default, but publication can be disabled C. User generated content can be published to the service, but publication is optional D. User generated content can be published to the service, but publication is optional and must be approved by a designated school/organisation based approver E. User generated content cannot be published to the service	
PF21	In relation to the content libraries available within the service, select all that apply.		A. Educational or curriculum aligned content and activities B. Non-educational content and activities C. Template libraries (e.g., presentations, web design, surveys etc.) D. Image, video and audio libraries E. User generated content F. Service provider generated content G. Search results that are not filtered based on user characteristics (e.g., age, year level, user type etc.) H. Unmoderated content (i.e., content is published to libraries without a review and/or approval process) I. None of the above	
PF22	Which of the following controls are/can be applied to the content library functionality available within the service, to ensure users are not exposed to information, including		A. The service moderates user generated content and reserves the right to remove	

	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, racism, sexism, etc.); and/or • Inappropriate for users under 18 years? Select all that apply.		content and/or users that breach the Terms of Use B. The service partly moderates user generated content through a profanity filter and/or human intervention C. The service has an implemented assurance procedure to ensure content conforms to quality standards prior to publication D. Users can report inappropriate user generated content E. Other F. No controls are applied	
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 E. Notifications can be via push notifications	
PF24	Which of the following controls are/can be applied to the notification and alert functionality. Select all that apply.		A. Notifications and alerts can be disabled by an administrator/moderator B. For each notification and/or alert, the school and/or users can specify and/or limit the audience C. 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 D. None of the above	
PF25	In relation to the online learning activities and/or game functionality available within the service, select all that apply.		A. The service generates online learning activities and/or games designed to assess socio-emotional factors (e.g., physical and mental health, well-being, behaviour) B. The service provides diagnostic and/or standardised testing	

			C. The user can create their own online learning activities and/or games. D. Answers can include pre-defined response options (e.g., multiple choice, Likert scales etc.) E. Answers are numerical free text fields (e.g., 0-9) F. Answers are short response free text fields (e.g., typing, equations, units of measurement, spelling and vocabulary) G. Answers can include long response free text fields (e.g., sentences, paragraphs, essays etc.) H. Data analysis, analytics and/or reporting is generated for users based on their responses/performance I. Data analysis, analytics and/or reporting is generated for teacher/school/administrator based on user responses/performance J. Data analysis, analytics and/or reporting can be distributed to parents using functionality within the service. K. Other	
PF26	Select the response option which best describes the publication of student results to the service. Publication means visible to all members and/or visitors to the service.		A. Student results cannot be published to the service. B. Student results are published to the service by default and publication cannot be disabled. C. Student results are published to the service by default, but publication can be disabled. D. Student results can be published to the service, but publication is optional.	
PF27	Select the functionality that is offered by the service. Select all that apply.		A. Customer relationship management B. Online ordering C. Payment processing D. Online bookings E. Subject selection F. Roll marking G. Class formation	

			H. Absence reporting and notifications I. Timetabling J. Workflow management and approvals K. Ticketing systems and service requests L. Records management M. Academic reporting N. Other O. 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 - would reasonably be provided to / collected by the service when used for its intended purpose?		A. Protection details B. Legal custodian arrangements C. Out of home care status 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 - would reasonably be provided to / collected by the service when used for its intended purpose? For each data asset, please specify whether it relates to student, staff, or parent. Select N/A if 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 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	
PF31	What, if any, other data not listed above would reasonably be disclosed to or collected by the service if used for its intended purpose? Please specify if data relates to student, staff or parent.		Free text field (informational)	

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, 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, OneRoster)?	1 & 2	Collected for reference only

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
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 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	Collected for reference only

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 vendor 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
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	T2
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

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, HR1, T1, T2, T3, T6, Q5, D3, D4, CC2, PR1, PR2, PR10, PR12, PR13, PR14, PF7, PF9

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

All of these questions have nominated preferred responses (with relevant tier indicators), with the exception of PF7 and PF9:

- PF7: In relation to the remote access tools available within the service, select all that apply.
  If "Remote access sessions are not logged" is selected, this will lead to a "non-compliant" assessment outcome.
- PF9: In relation to the chat / instant messaging functionality available within the service, select all that apply.
  If all three of the following response options are selected, this will lead to a "non-compliant" assessment outcome:
  - Users can chat/message with non-members (i.e., no log in is required to participate in chat/messaging).
  - Chat/instant messaging is unmoderated.
  - Chat/instant messaging is not logged.

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 2020.2):

The following is a list of the key changes to the ST4S Criteria for 2021.1:

Current criteria ID	Change	Question/Answer
P14	New	Accessibility question added
H1	Minor	Answer options updated
H2	Minor	Question text updated
H3	Minor	Question text updated
H5	Non-compliant (T1)	Question and answer options updated, added to non-compliant set
H6	New	Question regarding IRAP assessment of cloud services added
S1	Moderate	Updates to question and answer options
S2	Minor	Updates to answer options
S3	Moderate	Updates to question and answer options
S4	Moderate	Updates to question and answer options
S5	Minor	Question text updated
S6	Minor	Answer options updated
S9	Major	Question text significantly updated and answer options updated
S10	Moderate	Question and answer options updated
S11	Minor	ISM references updated
S13	Moderate	Question and answer options updated
L1	Minor	Question text updated
L2	Minor	Updates to question and answer options
A2	Major	Question text and answer options significantly updated
A3	Minor	Question text updated
A5	Minor	Question text updated
A7	Major	Question added to non-compliant list
A9	Minor	Question text updated
A11	New	New password reset question. Added to non-compliant list.
A12	New	New 3rd party account registration / login question added
A13	New	New question re: Default user access permissions added. Added to non-compliant list.
HR1	Minor	Question text updated, added to non-compliant list.
HR2	Minor	Question text updated
T2	Minor	ISM reference updated

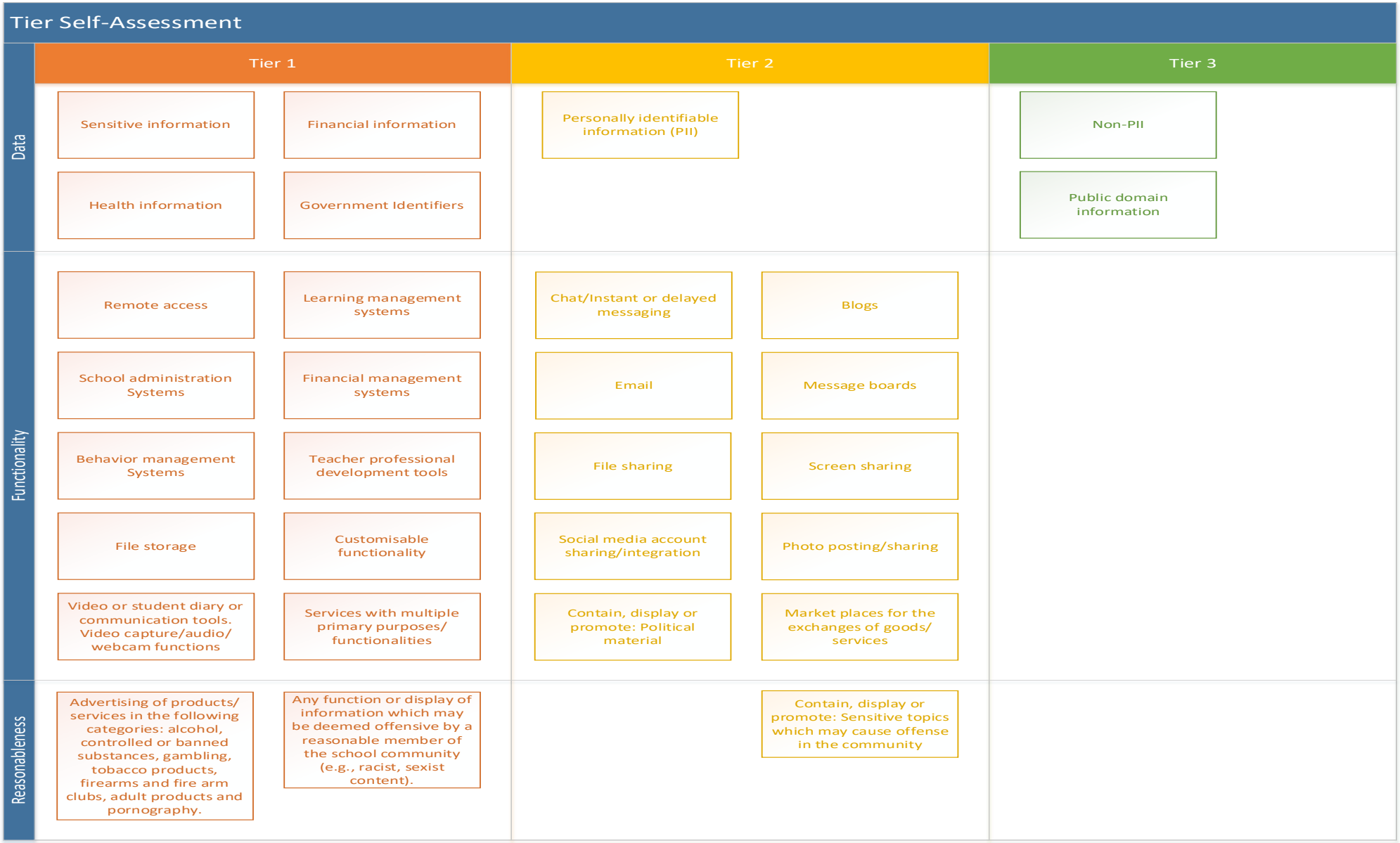
T8	Minor	ISM reference updated
Q2	Minor	Question text updated
Q3	Minor	Question text updated
Q4	Minor	Updates to question and answer options
Q5	Moderate	Updates to question and answer options
Q6	Minor	ISM reference updated
Q7	New	Security policy question added
G01	New	Governance question added
G02	New	Governance question added
G03	New	Governance question added
PR14	New	Search and directory functionality question added
PF14	Minor	Answer options updated

Appendix A – Tier Self-Assessment

The breadth and depth of an assessment performed on a vendor'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.



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 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

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 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	Personally identifiable 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 (eg. 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 permit, details of referees, marital status, record of interview, leave

1) Data		
Assessment Tier	Data Definitions	Data examples
		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; o Services with multiple primary purposes/functionalities (e.g., combination of those listed in Tier 2)	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)
Tier 2	Products which offer functionality in any of the following categories will be deemed as falling into tier 2:	Products which may contain, display or promote the following categories of information 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 (eg Facebook, Google) o Market places for the exchanges of goods/services	o Political material o Sensitive topics which may cause offense in the community
Tier 3	N/A	N/A