GESS

Global Education Security Standard

Controls for Education Services

Access 4 Learning Community

Global Education Security Standard (GESS) is a matrix/crosswalk of all existing security frameworks along with the core set of controls applicable to PK-20 data.

With the range of technical, functional, cyber security, data protection, privacy and other requirements, it is increasingly laborious to demonstrate compliance during procurement exercises.

With the growing number of security standards and frameworks, there is a significant amount of crossover, and much of it not in a language that allows for consideration of educational or operational needs of educational institutions. GESS streamlines this process by identifying and cross walking security controls that are applicable in Educational Technology products.

Building on the success of the ST4S assessments across Australia and New Zealand, the Student Data Privacy Consortium has brought together a working group of educational departments, leading vendors and academics to develop a Global Education Security Standard, to provide a common grounding baseline for all, as well as regional requirements.

More About GESS

GESS is an internationally agreed upon set of security controls pulled from major cyber security frameworks that are most applicable to the PK20 education ecosystem.

By joining the GESS subscribers you will be aiding the movement of the EdTech industry towards one common set of security controls to apply across many jurisdictions, thus avoiding the need to prove certification in multiple frameworks PK20 schools and districts are adopting the GESS set of controls as the expected security measures to be in place to protect all student data.

In the US the National Data Privacy Agreement V2 includes the GESS as an approved and accepted control framework. In Australia & New Zealand the preexisting ST4S controls are embedded within GESS.

GESS will streamline both the providers' ability to implement required security controls while at the same time meeting school expectations all with one common set of controls.

Release: 2.0
Date of this version: August 4, 2024
Author: GESS Project Team

GESS Disclaimer

The Global Education Security Standard ("GESS") is an identified set of security controls taken from relevant standards and legislation intended to be employed by marketplace providers in the Educational Technology field. Adherence to the usage conditions outlined in the GESS does not guarantee information security and user safety while using the online service. Users should always exercise caution when using online services and contact their local support team for assistance if required.

THE GLOBAL EDUCATION SECURITY STANDARD IS PROVIDED "AS IS." A4L MAKES NO WARRANTY OF ANY KIND, EXPRESS, IMPLIED, IN FACT OR ARISING BY OPERATION OF LAW, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND DATA ACCURACY. A4L NEITHER REPRESENTS NOR WARRANTS THAT THE OPERATION OF THE GESS PORTAL SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ANY DEFECTS WILL BE CORRECTED. A4L DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE SOFTWARE OR THE RESULTS THEREOF, INCLUDING BUT NOT LIMITED TO THE CORRECTNESS, ACCURACY, RELIABILITY, OR USEFULNESS OF GESS.

You are solely responsible for determining the appropriateness of using and distributing the GESS and you assume all risks associated with its use, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and the unavailability or interruption of operation. This GESS is not intended to be used in any situation where a failure could cause risk of injury or damage to property.

Commonly Used Terms

The following are commonly used terms throughout this document:

Your organization: The organization responsible for producing the product being evaluated (as a software producer).

Vendor: The organization responsible for producing the product being evaluated (as a commercial entity)

Sub-contractor: Other organizations, engaged by your organization in the process of producing or supporting the product being evaluated. Also referred to as sub-processors.

Independent third party: A supplier of goods and services other than your organization or its sub-contractors.

IT: Information technology

ICT: Information and communications technology (i.e. telephones and audiovisual devices, as well as computers and computer infrastructure)

Country of assessment: The country in which the assessment is being undertaken, on behalf of school authorities in that country

Data Controller: The organization(s) who decide the purpose and means of processing

Data Processor: Organization or body which processes personal data on behalf of the data controller.

Personal Data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Anonymous data: Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, and cannot be re-identified.

Data De-identification: A Visual Guide to Practical Data De-Identification (fpf.org) gives a good overview of the different stages. Will look for suitable terms for this and anonymisation

Anonymisation: As above

Transfer: The movement of personal data for processing or the intention of processing, from the customer to your organization/the vendor, or from your organization

Data Processing Agreement / Privacy Policy: A clear agreement between Your Organization / the Vendor and the customer, establishing what personal data is processed and other statutory information as set out by the customer's region (e.g. location, security information, retention, transfers)

Structure

The GESS controls are presented in the following categories; Governance, Personnel, Supply Chain, Asset & Risk Management, Access Control, Platform Security, Data Security, Detect & Respond, Privacy, Safeguarding, Product Information, Product Functionality. Within each category controls from various frameworks are grouped together into "Control Sets" and presented with a single control statement or requirement.

The Core Control Sets are presented first. At the end of the Core Control Sets a Supplemental list of control sets with associated questions or statements are provided. These are intended to gather more detailed information on each product that may be required for some jurisdictional specific assessments that may be based upon the functions of products or sensitivity of the data collected.

Core Control Sets

Governance

Establishes the framework and policies for organizational decision-making and accountability.

#	Control Statements	Standard/Controls
GO01	During development of the service, different mission, testing, auditing, and system support roles are allocated to different individuals (organization staff, vendor staff, external contractors, associates) as a matter of policy.	NIST 800-171 3.1.4 NIST 800-171 3.1.9 UKCE A7.4
GO02	There exists within the organization a position responsible for information security (i.e., CIO, CTO, CISO).	AUISM 714 NZISM 3.2
GO03	There exists within the organization a position responsible for privacy (i.e., CIO, CTO, CISO, Privacy Officer, Data Protection Officer).	
GO04	Security and privacy requirements are factored into the organization's planning and budget and there a discrete line item in the budget for security and privacy.	NIST 800-53 SA-2
GO05	Your organization's information security policy documents and implements the following minimum requirements: management's support for information security, compliance with laws and regulations, information security roles with corresponding responsibilities, access controls for sensitive information aligned with roles, retention period for security logs, regular policy reviews and updates in response to security incidents, logging of specific events, incident response policies with a roadmap for implementation if needed, personnel security, physical and environmental protections, system boundaries and connections to other systems, and policies for preserving system and information integrity including monitoring.	AUISM 1478 NIST 800-171 3.12.4 NIST 800-171 3.3.1 NIST 800-171 3.3.3 NIST 800-53 AC-1 NIST 800-53 AU-1 NIST 800-53 IR-1 NIST 800-53 PE-1 NIST 800-53 PS-1 NIST 800-53 SI-1 NZISM 5.1 NZISM 5.2

Governance

Establishes the framework and policies for organizational decision-making and accountability.

#	Control Statements	Standard/Controls
GO06	The organization has a documented and implemented security planning policy that outlines the following at a minimum: • management direction and support for planning around security; • requirement to comply with applicable laws and regulations; • policy that governs the development of security-related plans in the organization overall • requires coordination around the plans with other business units within the organization as appropriate; and • is the policy reviewed regularly and in response to security incidents.	NIST 800-53 MA-1 NIST 800-53 PL-1 NIST 800-53 PL-2(3)
GO07	The organization has a documented and implemented systems and services acquisition policy that outlines the following at a minimum: • management direction and support for planning around systems and services acquisition; • requirement to comply with applicable laws and regulations; • policy that governs the acquisition of resources, including: security and privacy requirements and acceptance criteria; • requiring the developer of the system or service to provide: • a description of the functional properties of any security controls; relevant design and implementation information for security controls; • a listing of all functions, ports, protocols and services in use; conformance with NIST FIPS-201-3 for any Personal Identity Verification functionality (smart card or equivalent for access to premises) • requirement for administrator documentation covering addressing in configuration, use and maintenance, and known vulnerabilities; • requirement for user documentation covering security and privacy functionality they can access, secure user interaction, and user responsibilities; • logging of attempts to obtain documentation that have been unsuccessful; and • is the policy reviewed regularly and in response to security incidents.	NIST 800-53 PL-1 NIST 800-53 PL-2(3)

Governance

Establishes the framework and policies for organizational decision-making and accountability.

#	Control Statements	Standard/Controls
GO08	A documented and implemented security policy is in place that governs the management and connectivity of mobile devices, including • use of a Mobile Device Management solution applied to all mobile devices and • encryption of any sensitive information transferred to mobile devices	CIS 3.6 NIST 800-171 3.1.18 NIST 800-171 3.1.19 NZISM 21.1 NZISM 21.4
GO09	A documented and implemented security policy is in place that governs the management and use of externally owned systems and devices, such as personally owned computers, portable storage devices and removable media (including media used for system maintenance); and includes: • physically controlling and securely storing all media (paper and digital) containing sensitive data; • restricting access to media containing sensitive data to authorized staff; • encrypting any sensitive data on media that is moved outside secure areas (including external work sites and work from home); • logging any transport of media outside secure areas; • marking media containing sensitive data with applicable distribution limitations; • requiring all removable portable storage devices to have an identifiable owner • disabling all autorun and auto-play functionality on removable media	CIS 10.3 NIST 800-171 3.1.20 NIST 800-171 3.10.6 NIST 800-171 3.7.4 NIST 800-171 3.8.1 NIST 800-171 3.8.2 NIST 800-171 3.8.4 NIST 800-171 3.8.5 NIST 800-171 3.8.6 NIST 800-171 3.8.7 NIST 800-171 3.8.8 UKCE A5.1 UKCE A5.3 UKCE A8.1 UKCE A8.2 UKCE A8.3 UKCE A8.4 UKCE A8.5

Personnel

Involves the management of human resources, focusing on recruitment, training, and retention to support organizational goals.

#	Control Statements	Standard/Controls
PE01	All vendor staff, external contractors and associates who have access to user data or user content undergo employment screening (e.g., criminal history checks, working with children checks) as per applicable regulatory requirements.	AUISM 434 NIST 800-171 3.9.1
PE03	Agreements are required to be signed by vendor staff, external contractors and associates who have access to user data or user content; the individuals are required to re-sign those agreements when they are updated; and those agreements provide for sanctions for failure to comply; and there is formal notification given when a sanctions process is initiated.	NIST 800-53 PS-8

Personnel

Involves the management of human resources, focusing on recruitment, training, and retention to support organizational goals.

#	Control Statements	Standard/Controls
PE04	The organization runs, based on the staff member's role, a customized security, privacy and online safety awareness/ education program which addresses the following: • Identification of who the awareness training needs to be delivered to, with records kept of training for each individual; • Identification, documentation and monitoring 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.); The content to be delivered for each awareness session such as: • Basic understanding of the need for information security, privacy and online safety, including causes of unintentional data exposure; • Actions to maintain security, privacy and online safety, including practical office/desktop practices; • Actions to respond to suspected security, privacy and online safety incidents; • Applicable policies and laws; • Practical security, privacy and online safety awareness exercises; • Data identification and storage, including the safe transfer of data, archival and destruction; • Disciplinary actions for significant security and privacy breaches by staff; • How to recognize and report indicators of potential insider threats to security by staff; • Covers recognizing social engineering attacks such as phishing, pre-texting and tailgating; • and Covers authentication best practices including MFA, password composition and managing credentials; • Covers verifications and reporting of out-of-date software patches and any failure in automated processes and tools; • and Covers the dangers of connecting to, and transmitting data over insecure networks for business activities, with specific training for remote workers regarding safe configuration of home networks.	AUISM 252 CIS 14.1 CIS 14.2 CIS 14.3 CIS 14.4 CIS 14.5 CIS 14.6 CIS 14.7 CIS 14.8 NIST 800-171 3.2.1 NIST 800-171 3.2.2 NIST 800-171 3.2.3 NIST 800-53 AT-4 NZISM 3.2 NZISM 3.3 NZISM 7.1 NZISM 9.1

Personnel

Involves the management of human resources, focusing on recruitment, training, and retention to support organizational goals.

#	Control Statements	Standard/Controls
PE05	There is documented and implemented process to remove access to systems, applications and data repositories for personnel (vendor staff, external contractors and associates) that no longer have a legitimate requirement for access (implemented on the same day); and are detected undertaking malicious activities (implemented immediately).	AUISM 1591 AUISM 430 NZISM 16.1 NZISM 16.4
PE06	The organization has a documented and implemented security training and awareness policy that outlines the following at a minimum: • management direction and support for information security; • requirement to comply with applicable laws and regulations; • security training and awareness processes to be adopted; • a requirement for communication to management to ensure they maintain an awareness of, and focus on, addressing privacy and security issues, and the policy is reviewed regularly and in response to security incidents.	NIST 800-53 AT-1

Supply Chain

Protects the integrity, confidentiality, and availability of the entire supply chain process by identifying and mitigating cyber threats and vulnerabilities from suppliers to end users.

#	Control Statements	Standard/Controls
SU02	If the service creates accounts in third party services, enforceable written agreements are in place with all of these third-party services covering this arrangement.	
SU03	Your organization implements real time security and privacy monitoring.	
SU06	Customers are notified in advance of any relocation or expansion (i.e. change of country) of: • the cloud infrastructure, including system components, user data and related data; and • any person (vendor or cloud infrastructure staff, external contractors or associates) with access to unencrypted customer data or any person with a means of accessing or extracting unencrypted data (e.g., those with access to encryption keys and encrypted customer data).	AUISM 1578 NZISM 12.7 NZISM 22.1

Supply Chain

Protects the integrity, confidentiality, and availability of the entire supply chain process by identifying and mitigating cyber threats and vulnerabilities from suppliers to end users.

#	Control Statements	Standard/Controls
SU07	Any cloud service providers that the service depends on have a recognized independent security audit and/or certificate of compliance such as ISO27001, SOC 2 Type II, FEDRAMP (NIST) or IRAP.	AUISM 1570 UKCE A2.9
SU08	• The Organization has an inventory of all third-party service providers; • regularly assess and manage the risks associated with these third-party providers; has contractual agreements in place to ensure third-party providers adhere to your information security and privacy policies; • ensures that the contractual agreements include notification of the transfer or termination of any personnel authorized to use your organization's systems; • monitors third party providers for compliance; • has defined and documented roles and responsibilities with regard to third party providers, including oversight of compliance • has a classification system for these third party providers; and • has a designated internal organization contact for each provider	CIS 15.1 NIST 800-53 PS-7 NIST 800-53 SA-9 NZISM 12.7 UKCE A2.9
SU09	Your organization seeks to absolve indemnity from any legal liabilities with regards to the operation of the service.	
SU12	Your organization has a current insurance policy of at least $1M with claims for data breach/loss.	UKCE A3.1 UKCE A3.2 UKCE A3.3 UKCE A3.4
SU13	This service relies on another IT service to operate as intended, such as using YouTube embeds or requiring Facebook logins. Specifically, it utilize third-party or outsourced components like plugins, browser extensions, hosting services, video streaming platforms (e.g., YouTube, Vimeo), image hosting services, or publishing services.	NZISM 12.7 UKCE A2.9
SU14	Terms of service/use are made available free of charge, and, published on the Internet or provided to customers prior to use of the service.	NIST 800-171 3.1.9
SU17	Per the terms of service, users are forewarned in the event the service provider wishes to terminate their account.	
SU20	Written agreements are in place with any third party who may receive data from the service that enforce data privacy and security standards at least as strict as those committed in agreements with customers.	NIST 800-53 CA-3
SU23	Your organization monitors compliance of third party providers which make up your solution for compliance with your organization's security and privacy requirements.	

Access & Risk Management

Identifies, evaluates, and mitigates risks to protect and optimize the use of organizational assets.

#	Control Statements	Standard/Controls
AM06	The responsibility for and ownership and accountability of critical system assets has been assigned to individual/s in the organization.	NZISM 3.4
AM09	Your organization has a documented and implemented security, privacy, and online safety risk management framework along with supporting processes. This framework includes: • scope and categorization of information assets and systems, • periodic or continuous risk assessments including those related to the supply chain, • implemented controls recorded in a risk register with details such as identified risks, • categories, • risk ratings, • owners, • mitigation actions, • accepted risks, • and residual risk ratings post-mitigation. It also includes proactive monitoring and testing of assets and systems to maintain security posture, with regular reviews and updates in response to security incidents.	AUISM 1526 AUISM 1636 NIST 800-171 3.11.1 NIST 800-53 CA-1 NIST 800-53 RA-1 NIST 800-53 SC-1 NZISM 3.2 NZISM 3.3 NZISM 4.1
AM11	The organization has a documented and implemented IT Asset management process including: • A register of all components that make up the service, including software, databases, middleware, infrastructure etc (their version numbers, patch levels, configuration, network address (if static), hardware address, machine name, asset owner, asset department, approval for connecting to the organization's network. For software the publisher, installation date, business purpose, URI, deployment mechanism, decommission date); • 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 sanitizing/removal of any data or secure destruction/ shredding); • A register of all baseline configurations associated with components, that is updated in line with the organization's system hardening process, with each component tracked only once. • Documentation of security and privacy impacts of asset changes; and • Removal, denial of access or the quarantining of any identified unauthorized assets on a regular basis.	AUISM 336 CIS 1.1 CIS 1.2 CIS 2.1 NIST 800-171 3.4.1 NIST 800-171 3.8.3 NIST 800-53 CM-1 NIST 800-53 CM-9 NIST 800-53 SA-10 NZISM 12.6 NZISM 13.4 NZISM 13.5 NZISM 13.6 NZISM 8.4

Access Control

Regulates who can view or use resources within an organization by managing permissions and authentication.

#	Control Statements	Standard/Controls
AC01	All users identified by individual identifiers assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device. [SP 800-63-3] provides guidance on digital identities.	AUISM 414 NIST 800-171 3.5.1 NZISM 16.1 UKCE A4.10 UKCE A4.2 UKCE A4.4 UKCE A4.5 UKCE A4.8 UKCE A4.9 UKCE A5.10 UKCE A5.9 UKCE A7.1 UKCE A7.10 UKCE A7.12 UKCE A7.14 UKCE A7.2 UKCE A7.3 UKCE A7.4 UKCE A7.7
AC02	All internal organization 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. If on a mobile device are all internal organization systems configured with a session or screen lock that activates after a maximum of 2 minutes of user inactivity or if manually activated by the user. In both cases requires the user to reauthenticate to unlock the system.	AUISM 428 CIS 4.3 NIST 800-171 3.1.10 NZISM 16.1 UKCE A5.10
AC03	User log-in sessions automatically terminated after a period of inactivity, or in response to a security incident.	NIST 800-171 3.1.11 UKCE A5.9
AC04	When a password reset is requested by the user or enforced 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.	AUISM 1227 AUISM 1593 AUISM 1594 AUISM 1595 NIST 800-171 3.5.9 NZISM 16.1 UKCE A5.3 UKCE A5.6

Access Control

Regulates who can view or use resources within an organization by managing permissions and authentication.

#	Control Statements	Standard/Controls
AC05	When a new password is selected by a user, there a restriction on both how similar the new password is to the previous password and the time duration or number of password changes before a previous password can be reused by a user.	NIST 800-171 3.5.7 NIST 800-171 3.5.8 UKCE A7.10 UKCE A7.11 UKCE A7.12
AC07	Default user access permissions set to deny unless specifically approved based upon a need to know rule.	UKCE A7.4
AC08	Within your organization and within the service super user privileged accounts restricted to specific users or roles.	NIST 800-171 3.1.5 NIST 800-171 3.1.7 UKCE A7.6 UKCE A7.7 UKCE A7.8 UKCE A7.9
AC09	Within your organization and within the service super user privileged accounts restricted by policy to only those functions that require such access and only for the duration required.	NIST 800-171 3.1.6 NIST 800-171 3.7.5 UKCE A7.4 UKCE A7.6 UKCE A7.7 UKCE A7.8 UKCE A7.9
AC10	In your organization, data access control lists implemented and configured based on a user's need to know and are these controls applied to local and remote file systems, databases and applications.	CIS 3.3
AC11	The service supports Single Sign-On (SSO)	
AC13	All access to the service requires authentication including both human and automated access.	NIST 800-171 3.1.1 NIST 800-171 3.5.2

Access Control

Regulates who can view or use resources within an organization by managing permissions and authentication.

#	Control Statements	Standard/Controls
AC14	Within the organization, All accounts are disabled after 45 days of inactivity and are user identifiers blocked from reassignment to new users for a defined period of time.	CIS 5.3 NIST 800-171 3.5.5 NIST 800-171 3.5.6 UKCE A4.6 UKCE A7.3
AC15	Within the organization there an inventory of all user, administrator and service accounts, which includes details of the person's name (if applicable), username/identifier, start/stop dates, and department (if an employee), and is this inventory of accounts validated at least every 3 months.	CIS 5.1 UKCE A7.1 UKCE A7.4 UKCE A7.6 UKCE A7.7 UKCE A7.8 UKCE A7.9
AC16	Are all passwords used to access the service (i.e. user, system, and privileged account passwords) protected in line with the recommendations of at least one of: the Australia Cyber Security Centre Information Security Manual; New Zealand Information Security Manual and/or Open Web Application Security Program's Application Security Verification Standard V2.4 Credential Storage Requirements, including the recommendation for ensuring passwords are hashed, salted and stretched?	NIST 800-171 3.5.10 NZISM 16.1
AC17	All user passwords masked or obscured as users enter then to access the service.	NIST 800-171 3.5.11
AC18	If using single factor authentication, password requirements a minimum of 14 characters with complexity and if using multi-factor authentication passwords are a minimum of eight characters with complexity for vendor staff, external contractors or associates with access to your organization's systems and the service.	AUISM 1559 AUISM 421 CIS 5.2 NIST 800-171 3.5.7 NZISM 16.1 UKCE A7.10 UKCE A7.11 UKCE A7.12 UKCE A7.13 UKCE A7.14 UKCE A7.16 UKCE A7.17
AC19	User passwords are reset after several unsuccessful logon attempts.	NIST 800-171 3.1.8 UKCE A7.10 UKCE A7.11 UKCE A7.12 UKCE A7.13
AC20	The service offers multi-factor authentication for end users.	AUISM 974 NIST 800-171 3.5.3 NZISM 16.1 NZISM 21.4 UKCE A7.14 UKCE A7.16 UKCE A7.17

Access Control

Regulates who can view or use resources within an organization by managing permissions and authentication.

#	Control Statements	Standard/Controls
AC21	Multi-factor authentication relay-resistant (e.g. nonces, one-time authentication tokens) is in the service.	NIST 800-171 3.5.4
AC22	Multi-factor authentication is mandated for vendor staff, external contractors or associates accessing systems remotely (including acces to cloud systems); and system administrators, support staff and staff with privileged accounts.	AUISM 1173 CIS 6.4 CIS 6.5 NIST 800-171 3.1.15 NIST 800-171 3.5.3 NZISM 16.4 NZISM 16.7 NZISM 19.1 NZISM 21.4 UKCE A7.16
AC23	The service requires additional authorization protocols to execute privileged commands remotely, compared to on-site.	NIST 800-171 3.1.15 NIST 800-171 3.7.5
AC24	The service requires externally exposed enterprise or third-party applications to enforce multi-factor authentication.	CIS 6.3 UKCE A7.16
AC25	The service provides role-based access control (RBAC) and this is this process documented for all systems including the service.	NIST 800-171 3.1.1 NIST 800-171 3.1.2 NZISM 16.2 NZISM 16.4 UKCE A7.1 UKCE A7.4
AC26	All vendor staff, external contractors or associates with access to systems, applications and information including audit logs, validated and approved by appropriate personnel. Personnel are periodically reviewed, at least annually, and revalidated or revoked; reviewed and revalidated or revoked due to changes in role employment and/or inactivity, or are appropriate security notices provided when they access the system.	AUISM 1404 AUISM 405 AUISM 430 NIST 800-171 3.1.9 NIST 800-171 3.9.2 NZISM 16.3 NZISM 16.5 UKCE A7.3
AC28	Privileged system management is segregated from user functionality through different computers or different operating systems or do you use VPNs.	NIST 800-171 3.13.3

Access Control

Regulates who can view or use resources within an organization by managing permissions and authentication.

#	Control Statements	Standard/Controls
AC29	The following physical access controls are in place at the locations were data is stored: • No public access, Visitor access only for visitors with a need to know and with a close escort; • Restricted access for authorized personnel with appropriate security clearance; • Physical controls on the facility and its support infrastructure (e.g. locked wiring closets, wiretapping sensors); • Single factor authentication for access control using secure swipe card, biometrics, coded access, other; • Control and management of any physical access control devices, such as secure swipe cards. The security alarm system includes the following: • Physical surveillance (e.g. video cameras); • Logging of visitors and of any visitor activity, with reporting of any identified anomalies; • Logging of any physical access to locations where data is stored; and Logging of any delivery and removal of physical system components.	AUISM 1296 NIST 800-171 3.10.1 NIST 800-171 3.10.2 NIST 800-171 3.10.3 NIST 800-171 3.10.4 NIST 800-171 3.10.5 NZISM 8.1 UKCE A2.4 UKCE A4.2
AC30	There is a documented and implemented process to grant access to systems, applications and data repositories for new personnel (vendor staff, external contractors and associates) or when a user changes roles.	CIS 6.1
AC31	In relation to the file upload and sharing functionality available within the service, the following controls are implemented; A. Authors have control over who can view and/or edit their files B. Administrators (e.g., teachers) can restrict who can view and/or edit users' files C. Administrators can disable file sharing	
AC32	In relation to the content creation functionality available within the service, the following controls are implemented; A. Users can share their content (e.g., via direct urls) B. Users have control over who can view or edit their content C. Administrators can restrict who can view and/or edit users' content D. Administrators can disable sharing of users' content	
AC33	The service provides 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.	UKCE A7.1 UKCE A7.2 UKCE A7.3 UKCE A7.4

Access Control

Regulates who can view or use resources within an organization by managing permissions and authentication.

#	Control Statements	Standard/Controls
AC34	In relation to the remote access tools available within the service, the following controls are implemented; A. Remote access tools can be disabled by an administrator or moderator B. Remote access sessions can only be initiated with the agreement of the user C. Users can take back control during remote access sessions D. Users can terminate remote access sessions once initiated. E. Onscreen notification is displayed throughout remote access sessions F. Remote access sessions are logged	NIST 800-171 3.1.12 NIST 800-171 3.13.12 NIST 800-171 3.13.14
AC35	In relation to the screen sharing functionality available within the service, all of the following controls are implemented; A. Use of screen sharing functionality is disabled by default B. Screen sharing can be disabled by an administrator or moderator C. Screen sharing sessions are initiated and/or accepted by the user who is sharing their screen D. Screen sharing sessions are logged	
AC37	The organization has a documented and implemented identification and authentication policy that outlines the following at a minimum: • management direction and support for identification and authentication; • requirement to comply with applicable laws and regulations; • policy on user identifiers; • policy on passwords and password updates; • policy on one-factor and multi-factor authentication security and usage; and • is the policy reviewed regularly and in response to security incidents.	NIST 800-53 IA-1
AC38	The services web services, if any, are secured with valid digital certificates signed by a reputable certificate authority.	NIST 800-171 3.13.15 NZISM 17.1 NZISM 17.2
AC39	The organization has a standardized, documented key management process which describes the full lifecycle of each key used in the operation of the production environment.	NIST 800-171 3.13.10 NZISM 17.9

```
    @candidates   = observations - [control]
    evaluate_candidates

    freeze
  end

  # Public: the experiment's context
  def context
    experiment.context
  end

  # Public: the name of the experiment
  def experiment_name
    experiment.name
  end

  # Public: was the result a match between all
  def matched?
lib/scientist/result.rb  1:1
```

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS01	Within the organization all the following application controls are in place on all workstations and on all servers; • restricting the execution of drivers to an organization-approved set • implemented using cryptographic hash rules, publisher certificate rules or path rules • rule sets are validated on an annual or more frequent basis • when implementing application control using publisher certificate rules, both publisher names and product names are used • extended to tools and applications used in system and software maintenance	AUISM 1471 AUISM 1490 AUISM 1582 AUISM 1656 AUISM 1657 AUISM 1658 AUISM 843 AUISM 955 NIST 800-171 3.13.13 NIST 800-171 3.7.2 NZISM 14.2
PS02	Enterprise assets and software are securely managed via one or more of the following; Version controlled infrastructure as code or accessing administrative interfaces securely via SSH or HTTPS.	CIS 4.6
PS03	Vendor staff, external contractors or associates with non-privileged accounts are restricted from installing, uninstalling, disabling or making any changes to software and system configuration on servers and endpoints.	AUISM 1491 AUISM 1584 NIST 800-171 3.4.2 NIST 800-171 3.4.5 NIST 800-171 3.7.2 NIST 800-171 3.7.6 NZISM 14.1

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS04	The organization has a documented and implemented logging procedure, covering the collection, review and retention of logs, which is reviewed annually and which requires all systems in the organization (e.g., servers, storage, network, applications, etc.) to log the following and synchronize logs to a consistent time source: • Authentication logs (e.g., successful login, unsuccessful login, logoff) • Privileged operations logs (e.g., access to logs, changes to configurations or policy, failed attempts to access data and resources) • User administration logs (e.g., addition/ removal of users, changes to accounts, password changes) • System logs (e.g., system shutdown/ restarts, application crashes and error messages) • And uses or ascribes a unique identifier of the user who has performed the activity being logged.	AUISM 109 AUISM 1536 AUISM 1537 AUISM 585 CIS 8.1 NIST 800-171 3.1.7 NIST 800-171 3.3.1 NIST 800-171 3.3.2 NIST 800-171 3.3.7 NIST 800-53 AU-2 NZISM 16.6
PS05	The organization has implemented a centralized logging facility to store logs which: Ensure logs cannot be tampered with; Triggers an alert in case a logging transaction fails; Supports audit reduction and report generation for analysis; and Ensures adequate storage to comply with specified retention times.	AUISM 1405 CIS 8.3 NIST 800-171 3.3.1 NIST 800-171 3.3.4 NIST 800-171 3.3.6 NIST 800-171 3.3.8 NZISM 16.6 NZISM 18.4
PS06	The organization has 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 • Categorization of IT change (e.g., Standard, Pre-Approved, Emergency, etc.); • Approval requirements for each category of IT change; • Assessment of potential security impacts; • Prerequisites for the IT change (e.g., the IT change has been tested in a non-production environment); • Documentation requirements in regard to the change (e.g., completion of a template in an IT change management tool, completion of a rollback plan, etc.); • Documentation that needs to be updated as a result of the change (e.g., as-built documentation, IT Disaster Recovery Plans, etc.); • IT change communication processes (e.g., notifications to users); and • Validations are required for all changes to systems before they are finalized	AUISM 1211 NIST 800-171 3.4.3 NIST 800-171 3.4.4 NIST 800-53 CA-1 NIST 800-53 CM-3(2) NIST 800-53 SA-1 NZISM 6.3

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS07	The organization have a documented and implemented maintenance policy that outlines the following at a minimum: • management direction and support for maintenance; • requirement to comply with applicable laws and regulations; • governs the development of a maintenance plan for the organization's software, hardware, and firmware; • ensures that any software no longer supported with updates is either removed as unauthorized, or else documented as an exception with mitigating controls and risk acceptance; • ensures that only fully supported web browsers and email clients are allowed to execute in the enterprise; and the policy is reviewed regularly and in response to security incidents.	CIS 2.2 CIS 2.3 CIS 9.1 NIST 800-53 MA-1
PS08	The service's application development has the following characteristics: • Environments are separated into at least development, testing and production environments; • Development and modification of software only takes place in development environments; • Unauthorized access to the authoritative software source is prevented; • Secure-by-design principles and secure programming practices are used as part of application development. (This includes: integrating the organization's security and privacy risk management into application development; assigning responsibility for security and privacy as defined roles to individuals during application development); • Privacy-by-design principles; • Threat modeling is used in support of application development; and • Alignment to a security and privacy architecture that has been drawn up for the system	NIST 800-171 3.13.2 NIST 800-53 PL-8 NIST 800-53 SA-3 NZISM 14.4 NZISM 14.5

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS09	A documented and implemented system hardening process is in place which: • Includes in scope operating systems, virtualization platforms, storage, network, software, applications, workstations and other end-user devices (including portable, mobile and IoT devices); • Includes the management of default user accounts and access levels and the uninstallation or disablement of the unnecessary services; • Ensures only required ports, protocols, services and authorizations are enabled, whether for internal or external connections (all others are restricted); • Is reviewed annually and when significant changes occur, including when system components are installed or upgraded; • Results in security configurations being established and enforced for organization systems; • Ensures only required and authorized software is installed and used	AUISM 1406 AUISM 1585 AUISM 1588 AUISM 1605 CIS 2.3 CIS 4.1 CIS 4.2 NIST 800-171 3.13.6 NIST 800-171 3.14.7 NIST 800-171 3.4.2 NIST 800-171 3.4.6 NIST 800-171 3.4.7 NIST 800-171 3.4.8 NIST 800-171 3.4.9 NIST 800-171 3.7.3 NIST 800-53 CA-9 NIST 800-53 CM-2(1) NIST 800-53 CM-2(7) NZISM 14.1 NZISM 22.2
PS10	Enhanced security configurations are enforced for organization systems and components moving physically to high-risk areas or off-site for maintenance.	NIST 800-171 3.7.3 NIST 800-53 CM-2(7)

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS11	The following perimeter controls are in place: • External firewall; • Host based firewalls or port filtering on end-user devices with default-deny rules; • IDS/IPS (Intrusion Detection System/Intrusion Prevention System); • DMZ (Demilitarized Zone) for hosting external sites; • Content filtering (including blocking of unnecessary file types); • DoS/DDoS (Denial of Service/Distributed Denial of Service) defence; • Web Application Firewall (WAF); • Filtering and monitoring of outgoing traffic (spikes, unusual activity, malicious content); • Packet inspection; • Network segmentation; • VPN required for remote access; • Detection and monitoring of unauthorized devices on the network through both passive and active device discovery, resulting in updates to asset inventory on a regular basis; • DNS filtering and network URL based filters; and • Organization assets are configured to use trusted DNS servers • explicit restrictions on information transfer to external systems based on data structures and content, as well as authorization (for example, enforcing read-only access, filtering, message security tagging and reclassification of message security) • Authorization and encryption on the organization's wireless network • Restrictions on the use of portable storage devices to transfer information from organization systems to external systems • Blocking of split tunnelling • Automatic termination of inactive network connections at the end of a session or after a defined period of inactivity • Implemented traffic flow policy on each external telecommunications service used; Prevent unauthorized use of control plane traffic (e.g Border Gateway Protocol routing, Domain Name System) • Data origin authentication and Integrity verification on name/ address resolution services such as DNS, including child zone • Fault tolerance on name/address resolution services such as DNS, including secondary server and internal/external server separation • Periodic scan of organizational file storage and real-time scans of files from external sources • DNS filtering and network URL based filters; and	AUISM 1435 AUISM 1528 CIS 4.4 CIS 4.5 CIS 9.2 NIST 800-171 3.1.13 NIST 800-171 3.1.14 NIST 800-171 3.1.16 NIST 800-171 3.1.17 NIST 800-171 3.1.21 NIST 800-171 3.1.3 NIST 800-171 3.13.9 NIST 800-171 3.14.6 NIST 800-171 3.14.7 NIST 800-53 SC-7(3) NIST 800-53 SC-7(4) NZISM 10.8 NZISM 18.4 NZISM 19.1 NZISM 19.3 UKCE A2.8 UKCE A4.1 UKCE A4.10 UKCE A4.11 UKCE A4.12 UKCE A4.2 UKCE A4.3 UKCE A4.4 UKCE A4.5 UKCE A4.6 UKCE A4.7 UKCE A4.8 UKCE A4.9

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS11 (cont)	• Organization assets are configured to use trusted DNS servers • explicit restrictions on information transfer to external systems based on data structures and content, as well as authorization (for example, enforcing read-only access, filtering, message security tagging and reclassification of message security) • Authorization and encryption on the organization’s wireless network • Restrictions on the use of portable storage devices to transfer information from organization systems to external systems • Blocking of split tunnelling • Automatic termination of inactive network connections at the end of a session or after a defined period of inactivity • Implemented traffic flow policy on each external telecommunications service used; Prevent unauthorized use of control plane traffic (e.g Border Gateway Protocol routing, Domain Name System) • Data origin authentication and Integrity verification on name/address resolution services such as DNS, including child zone • Fault tolerance on name/address resolution services such as DNS, including secondary server and internal/external server separation • Periodic scan of organizational file storage and real-time scans of files from external sources	
PS12	Use of macros (e.g., Microsoft Office macros) and scripts (VB, java, PowerShell) is controls as follows: - internal use is blocked except for users that have a demonstrated business requirement; - macros and scripts in files originating from the internet are blocked; - macros and scripts are subject to antivirus scanning; and - macro and script security settings can’t be changed by users.	AUISM 1487 AUISM 1488 AUISM 1489 NZISM 20.3
PS13	All of the organization’s desktop computers, laptops, tablets, mobile phones and other devices are protected from viruses and malware by: Having anti-virus and anti-malware installed; Limiting the applications and services which can be installed to a documented approved set; Updating anti-virus and anti-malware signatures at least daily; Scanning files automatically before access; and blocking access to malicious sites before they are accessed.	CIS 10.1 CIS 10.2 CIS 10.3 NZISM 14.1
PS14	Production servers (e.g., authentication servers, Domain Name System (DNS), web servers, file servers and email servers), containers, serverless services and all end points protected by HIPS (Host-based Intrusion Prevention System), software-based application firewalls, anti-virus and anti-malware are all of kept up to date with definitions and maintained.	AUISM 1034 AUISM 1341 AUISM 1416 AUISM 1417 CIS 10.1 NIST 800-171 3.4.6 NZISM 14.1 NZISM 18.4

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS15	Internet facing components (e.g., web servers) are separated from other online components (e.g. databases) using the following controls: Secure communication between network segments (e.g., using firewalls), including filtering between network segments DMZ for internet-facing components and separate trusted zones for other components Virtual (e.g., VLAN) or physical network segregation.	AUISM 1006 AUISM 1181 AUISM 1182 AUISM 1364 AUISM 1436 AUISM 1437 AUISM 1479 AUISM 1532 AUISM 1577 AUISM 385 AUISM 520 AUISM 529 AUISM 530 AUISM 535 AUISM 628 NIST 800-171 3.1.3 NZISM 10.8 NZISM 14.1 NZISM 19.1 NZISM 22.2
PS16	Your organization use a centrally managed approach to patch, update or otherwise maintain applications, drivers, operating systems, and firmware and hardware which includes ensuring: • the integrity and authenticity of patches; • successful application of patches; • that patches remain in place; and • that the list of supported software for updates is reviewed regularly	AUISM 298 CIS 2.2 CIS 7.3 CIS 7.4 NIST 800-171 3.7.1 NZISM 12.4 NZISM 14.5 UKCE A6.4 UKCE A6.5
PS17	Patches, updates or vendor mitigations for security vulnerabilities in Internet facing services (including operating systems of Internet-facing services), workstation, server and network device operating systems; operating systems of other ICT equipment; drivers and firmware; are applied within two weeks of release, or within 48 hours if an exploit exists.	AUISM 1690 AUISM 1694 AUISM 1695 AUISM 1696 AUISM 1697 AUISM 1751 CIS 12.1 CIS 7.3 NIST 800-171 3.14.1 NZISM 12.4 UKCE A6.4 UKCE A6.5
PS18	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products are applied within two weeks of release, or within 48 hours if an exploit exists.	AUISM 1691 AUISM 1692 CIS 7.4 NIST 800-171 3.14.1 NZISM 12.4 UKCE A6.4 UKCE A6.5

Platform Security

Ensures the protection of hardware and software platforms from threats, vulnerabilities, and unauthorized access.

#	Control Statements	Standard/Controls
PS19	Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.	AUISM 1693 CIS 7.4 NIST 800-171 3.14.1 NZISM 12.4

Data Security

Protects sensitive information from unauthorized access, corruption, or theft throughout its lifecycle.

#	Control Statements	Standard/Controls
DS01	All data backups are stored for a minimum of 3 months.	AUISM 1511 NZISM 6.4
DS02	Deletion of data from the service is performed securely commensurate with the data's sensitivity and certified.	CIS 3.5 NZISM 13.1 NZISM 13.4 NZISM 13.5 NZISM 13.6 NZISM 22.1
DS03	Full restoration of backups is tested at least once initially implemented and each time major information technology infrastructure changes occur, (e.g., technology stack changes, vendor changes, or platform changes) or at least annually.	AUISM 1515 NZISM 6.4
DS04	Partial restoration of backups is tested on a quarterly or more frequent basis.	AUISM 1515 NZISM 6.4
DS05	There exists a documented and implemented data retention policy including: minimum data retention period; maximum data retention period; and the deletion of identifying or sensitive data no longer required.	CIS 3.4

Data Security

Protects sensitive information from unauthorized access, corruption, or theft throughout its lifecycle.

#	Control Statements	Standard/Controls
DS07	The organization has a documented and implemented Business Continuity Plan for the service, which is updated annually and when significant changes occur, covering: • Backup strategies (including automated backups at least weekly or more frequently as required and backups that are stored disconnected); • Restoration strategies (e.g., disaster recovery), including prioritization; • Preservation strategies; • And the security of backed up data.	AUISM 1510 AUISM 1547 AUISM 1548 CIS 11.1 CIS 11.2 NZISM 6.4
DS08	The organization has a documented and implemented data management policy that outlines the following at a minimum: • Identification of data assets; • recording of data assets in a data inventory; • data asset ownership; • tracking of data sensitivity; • handling of data procedures; • data retention limits; • disposal requirements informed by data sensitivity and retention standards; and • is reviewed and updated annually with a priority on sensitive data.	CIS 3.1 CIS 3.2
DS09	Data is protected in transit, including between the user, web applications and other system components, at minimum with the following encryption algorithms: Encryption: AES 192 GCM/CCM, CHACHA20 POLY 1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048+) FIPS 186-4, ECDSA (224+) using NIST P-384 curve or RSA (2048+); Key Exchange: DH (3072+), ECDH (256+) using NIST P-384 curve and/or RSA (3072+); Protocol: TLS 1.2 or above only (TLS 1.3 recommended)	AUISM 1139 AUISM 1277 AUISM 471 AUISM 994 NIST 800-171 3.13.11 NIST 800-171 3.13.15 NIST 800-171 3.13.8 NZISM 17.2 NZISM 17.3
DS10	Any non-production environments storing or processing production data have the same security controls as the production environment.	AUISM 1420 NZISM 14.4 NZISM 20.1 UKCE A2.7
DS11	Data is protected at rest, including backups, data storage and audit logs, at minimum with the following encryption algorithms: AES 192, AES 256 (AES 256 recommended).	NIST 800-171 3.13.4

Data Security

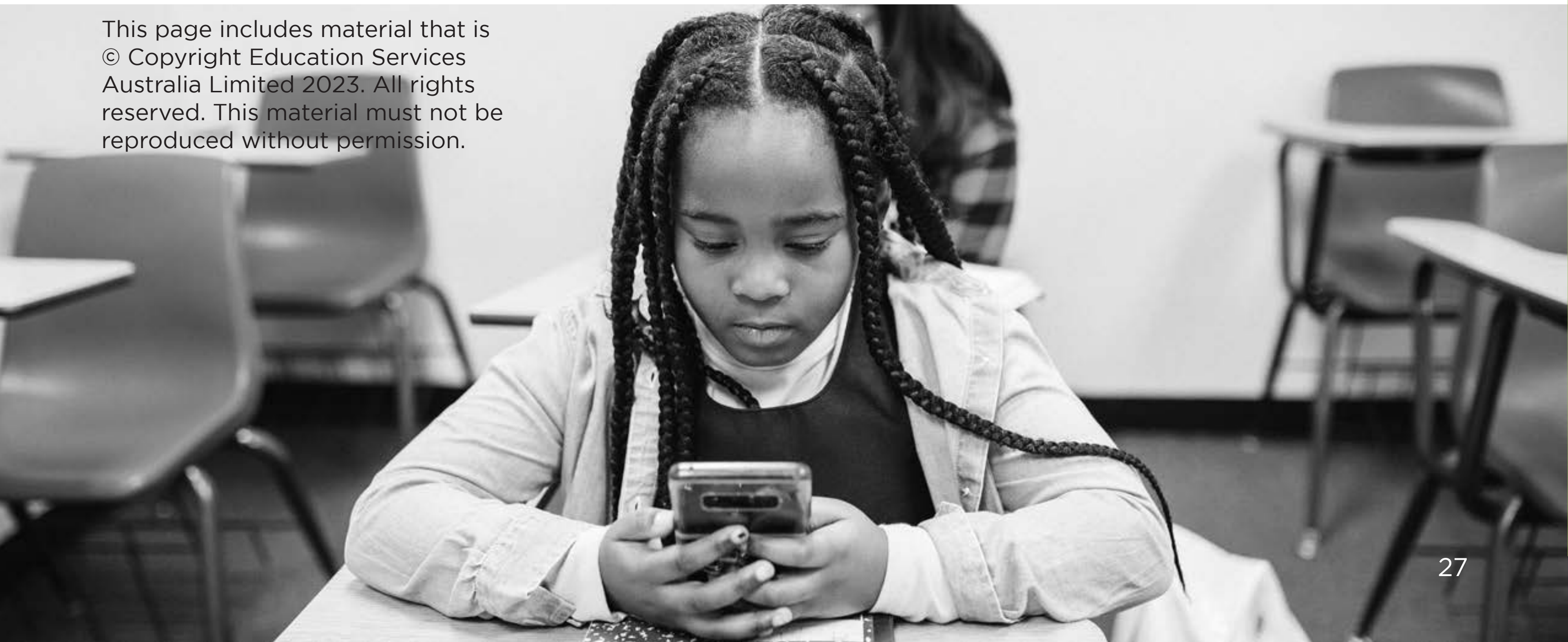
Protects sensitive information from unauthorized access, corruption, or theft throughout its lifecycle.

#	Control Statements	Standard/Controls
DS12	Unauthorized and unintended information transfer via unencrypted shared system resources, such as caches and hard disks is prevented.	AUISM 1139 AUISM 1759 AUISM 1761 AUISM 471 AUISM 472 AUISM 474 NIST 800-171 3.13.11 NIST 800-171 3.13.8 NZISM 17.2 NZISM 17.3
DS13	Customer data uploaded to the service, if any, is encrypted with an algorithm at least as strong as AES-192.	AUISM 1139 AUISM 1759 AUISM 1761 AUISM 471 AUISM 472 AUISM 474 NIST 800-171 3.13.11 NIST 800-171 3.13.8 NZISM 17.2 NZISM 17.3
DS14	If a multi-tenancy model is used to store and process customer data, partitioning controls are implemented to securely separate each customer's data from that of other customers.	AUISM 1436 NIST 800-171 3.1.3 NZISM 10.8 NZISM 22.2
DS15	Your organization enforces 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	AUISM 1246 AUISM 1247 AUISM 1249 AUISM 1250 AUISM 1260 AUISM 1262 AUISM 1263 AUISM 1273 NZISM 10.8 NZISM 14.4 NZISM 20.1
DS16	Network controls are in place to prevent system components that do not need to be accessed from the Internet from being accessed from the Internet.	NIST 800-171 3.13.1 NIST 800-171 3.13.5
DS18	System memory is protected from unauthorized code execution.	NIST 800-53 SI-16

Detect and Respond

Implements measures to identify security incidents promptly and orchestrates an effective response to mitigate damage.

#	Control Statements	Standard/Controls
DR01	The organization has a documented and implemented event log auditing procedure which outlines, at a minimum: • Schedule of audits (annual or real-time for sensitive data); • Definitions of security violations; • Actions to be taken when violations are detected; and • Reporting requirements.	AUISM 109 NIST 800-171 3.3.5 NIST 800-171 3.3.6 NIST 800-53 AU-6 NIST 800-53 CA-7 NZISM 16.6 NZISM 7.1
DR02	All relevant audit and logging data will be supplied to customers in response to customer requests.	
DR03	The following features built into the file download functionality available within the service: • All files are scanned for Malware/Viruses during download; • All files are scanned for Malware/Viruses while at rest; and • All files found to contain Malware/Viruses are deleted or quarantined.	AUISM 657 NIST 800-171 3.14.2 NZISM 14.1
DR04	The following features built into the file upload functionality available within the service; • All files are scanned for Malware/Viruses during upload • All files are scanned for Malware/Viruses while at rest • All files found to contain Malware/Viruses are quarantined or deleted.	AUISM 657 NIST 800-171 3.14.2 NZISM 14.1



Detect and Respond

Implements measures to identify security incidents promptly and orchestrates an effective response to mitigate damage.

#	Control Statements	Standard/Controls
DR05	The organization conducts vulnerability scans for production systems at least monthly. The organization conducts application penetration tests at least annually. The organization has a process in place to analyze identified security vulnerabilities to determine their potential impact, mitigate the vulnerabilities in a timely manner, and monitor the status of security vulnerability mitigation.	AUISM 1163 CIS 10.2 CIS 18.1 CIS 7.1 CIS 7.2 NIST 800-171 3.11.2 NIST 800-171 3.11.3 NIST 800-171 3.12.2 NIST 800-171 3.12.3 NIST 800-171 3.14.1 NIST 800-171 3.14.3 NIST 800-171 3.14.4 NIST 800-53 CA-7 NIST 800-53 RA-5(1) NIST 800-53 RA-5(2) NIST 800-53 SA-9(2) NIST 800-53 SI-4(5) NZISM 14.4 NZISM 14.5 NZISM 4.1 NZISM 4.3 NZISM 6.1 NZISM 6.2 UKCE A6.4 UKCE A6.5 UKCE A8.1 UKCE A8.2 UKCE A8.3 UKCE A8.4 UKCE A8.5
DR06	Your organization has a formal, documented and implemented incident response plan which requires security, privacy and online safety incidents to be: Identified, following a clear definition; Reported by staff (if internal); Proactively monitored; Contained; Investigated; Remediated; Tracked with metrics, to measure response effectiveness; and Recorded in a register with the following information at a minimum: Date incident occurred; Date incident discovered; Description of the incident; Actions taken in response to the incident; and Name of person to whom the incident was reported.	AUISM 125 CIS 17.2 CIS 17.3 NIST 800-171 3.6.1 NIST 800-53 IR-8 NZISM 22.1 NZISM 5.6 NZISM 7.1 NZISM 7.2

Detect and Respond

Implements measures to identify security incidents promptly and orchestrates an effective response to mitigate damage.

#	Control Statements	Standard/Controls
DR07	The incident response capability of the organization is regularly tested and reviewed.	NIST 800-171 3.6.3
DR08	As part of your organization's incident handling process your organization: • has one key person and at least one backup tasked with managing the organization's incident handling process; • and has contact information for all parties that need to be informed of security incidents (e.g. staff, third party vendors, law enforcement, insurance providers, government agencies etc); • and contacts are updated annually.	CIS 17.1
DR09	When a data breach occurs, affected customers, organizations, and the relevant authorities, are notified as soon as possible after a data breach is discovered and given all relevant details (including affected individuals and what information was disclosed).	AUISM 123 AUISM 140 AUISM 141 NIST 800-171 3.6.2 NZISM 7.2
DR10	When a data loss/corruption event occurs, affected customers and/or organizations are notified as soon as possible after this is discovered and given all relevant details.	AUISM 123 AUISM 140 AUISM 141 NIST 800-171 3.6.2 NZISM 7.2

Privacy

Ensures that personal data is collected, used, and protected in compliance with laws and regulations to safeguard individual privacy rights.

#	Control Statements	Standard/Controls
PR04	The registration of an account or use of the service generates a user 'profile' within the service, and if so, can visibility be restricted (e.g., made private or restricted to known users).	
PR07	The service logs the following events: • Creation • Access • Modification • Deletion of student and personal information.	
PR08	The privacy policy applicable to the service is made freely available to each customer prior to the customer's decision to purchase the service.	NIST 800-171 3.1.9

Privacy

Ensures that personal data is collected, used, and protected in compliance with laws and regulations to safeguard individual privacy rights.

#	Control Statements	Standard/Controls
PR09	The organization does not share user data with third parties in any circumstances other than the following: • the individual has consented to the use or disclosure of the information; • the use or disclosure of the information is required or authorized by or under a law or a court/tribunal order in the customer's country; • the use or disclosure is required or permitted under privacy legislation in the customer's country; or • the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body • relevant jurisdictional circumstances, for example for services in Australia, as per the Australian Privacy Principles, as well as the permitted general situations and permitted health situations. For services in New Zealand as per the Privacy Principles and information sharing provisions in the Privacy Act 2020, as well as the Oranga Tamariki Act 1989 and the Family Violence Act 2018. For the UK, as per Keeping Children Safe in Education.	NIST 800-171 3.1.22
PR10	Subscription to the service's commercial mailing list is opt-in by choice. 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.	

Privacy
Ensures that personal data is collected, used, and protected in compliance with laws and regulations to safeguard individual privacy rights.

#	Control Statements	Standard/Controls
PR11	The service does not 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 authorized by or under a law or a court/tribunal order within the customer’s country; • Use or disclosure is necessary for the organization to verify the identity of the individual for the purposes of the organization’s activities or functions; • Use or disclosure is necessary for the organization to fulfil its obligations to a government agency or education authority within the customer’s country; • Use or disclosure is required or authorized by or under a law or a court/tribunal order within the customer’s country; • The organization reasonably believes the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities; • The identifier, organization or circumstances are prescribed by regulations.	
PR12	The organization has a process which allows customers to request the service to provide access to, correct, or delete all personal information relating to them.	
PR15	The privacy policy for the service outlines 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.	

Supplemental Control Sets

The Supplemental Control Sets are intended to gather more detailed information on each product that may be required for some jurisdictional specific assessments that may be based upon the functions of products or sensitivity of the data collected.

Personnel

Involves the management of human resources, focusing on recruitment, training, and retention to support organizational goals.

#	Questions	Standard/Controls
PE02	Within your organization, please select the agreements that all vendor staff, external contractors and associates who have access to user data or user content required to sign?	NIST 800-53 PL-4 NIST 800-53 PL-4(1) NIST 800-53 PS-6 NIST 800-53 PS-8

Supply Chain

Protects the integrity, confidentiality, and availability of the entire supply chain process by identifying and mitigating cyber threats and vulnerabilities from suppliers to end users.

#	Questions	Standard/Controls
SU01	Does the service require, suggest or imply that accounts be created in any third-party services for any purpose whatsoever (data collection, data exchange, other)?	
SU04	Select the option which best describes where user data or any related data (e.g., metadata, logs, user content) is stored or processed across all components of the service, including live solution, backup, disaster recovery, test environment, and development environments.	AUISM 1452 NZISM 12.7 NZISM 22.1
SU05	From what countries do vendor staff, including support, administration, development and testing, and external contractors or associates, access user data and any related data (e.g., metadata, logs) collected or used by the service (including backups and recovery)?	NZISM 12.7 NZISM 22.1 UKCE A2.1 UKCE A2.2 UKCE A2.3
SU10	Are you the product or service's original developer, a re-seller or other?	
SU11	In what jurisdiction would disputes, regarding usage of the service, be handled? (e.g., Washington USA, Victoria Australia, New Zealand)	
SU15	As per the terms of service, what, if any, age restrictions apply to the use of the service?	
SU16	What are the specified definitions of intellectual property ownership, including copyright, in the terms of use for the service? (e.g., user generated content)? Include excerpt from terms of use.	
SU18	What, if any, third party products are used to provide the file upload and storage functionality within the service? Select all that apply.	
SU19	In relation to the data integration, aggregation, data broker, data hub, data distribution hub functionality, does the service (the collector of data/ data aggregator / data broker) assume ownership of any data transferred to, or transiting through, the service?	NIST 800-53 CA-3
SU21	Which security and privacy compliance certifications do recipient third party systems hold?	NIST 800-53 CA-3
SU22	When a data breach or data loss event occurs in third party recipient systems, who notifies the customer (e.g., school, school jurisdiction or school system)?	

Access & Risk Management

Identifies, evaluates, and mitigates risks to protect and optimize the use of organizational assets.

#	Questions	Standard/Controls
AM01	Select the compliance certifications or security assessments that have been completed for the service and your organization, or another organization contracted by you to perform the development, maintenance and/or support of your solution (excluding the infrastructure provider e.g., AWS, Azure, Sendgrid)	NIST 800-171 3.12.1 NZISM 5.8
AM02	Which compliance certifications or assessments do you complete on a regular basis (i.e. repeatedly)?	NIST 800-171 3.12.1
AM03	Which compliance certifications or assessments are undertaken by independent assessors?	NIST 800-171 3.12.1
AM04	Select the privacy related compliance certifications or assessments that have been completed for the service and your organization, or another organization contracted by you to perform the development, maintenance and/or support of your solution (excluding the infrastructure provider e.g., AWS, Azure, Sendgrid)	NIST 800-53 CA-2(1) NIST 800-53 CA-7(1)
AM05	If the solution processes electronic payments or holds credit card data is it Payment Card Industry Data Security Standards (PCI DSS) compliant?	NZISM 5.8
AM07	For the service being assessed, what is the deployment architecture used for customers?	
AM08	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 behavior incidents/discipline, behavioral observations/notes • Consent (e.g., collection and/or recording of consent) • Student absence details (i.e., records of attendance and reason for absence) • Records of contact (e.g., between parents, teacher, school, and/or student) and other agencies • Student/Learning support service information and support arrangements • Enrollment support records (sensitive case, complex case, adjustments, student plan, developmental map, transportation, Individual Education Plans, Oranga Tamariki ‘All about Me’ plan)	

Access & Risk Management

Identifies, evaluates, and mitigates risks to protect and optimize the use of organizational assets.

#	Questions	Standard/Controls
AM10	Are all service application developments assessed as per a security testing methodology that is consistent with the guidance provided by the latest industry standard frameworks (e.g., Open Web Application Security Project (OWASP) Testing Guide v4.2, Building Security In Maturity Model (BSIMM))?	AUISM 1239 NIST 800-53 SA-10 NZISM 14.4 NZISM 14.5

Access Control

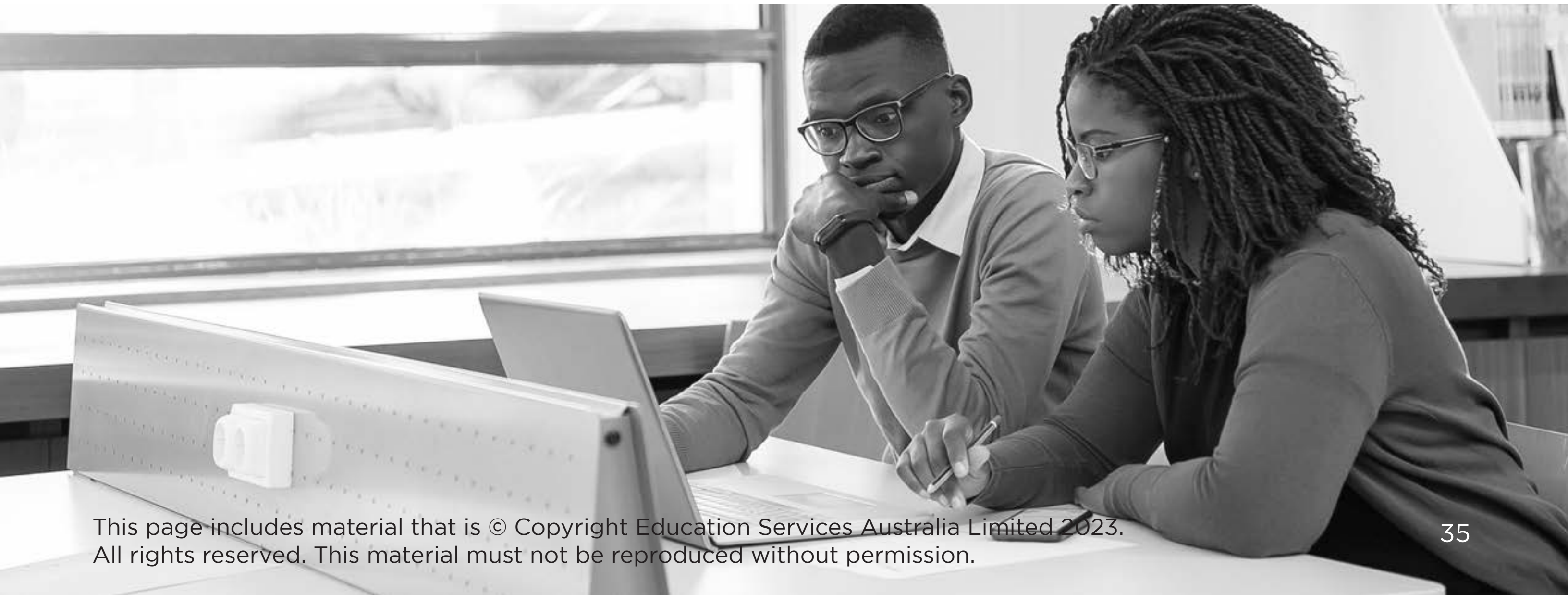
Regulates who can view or use resources within an organization by managing permissions and authentication.

#	Questions	Standard/Controls
AC06	The service allows user registration or logon/authentication or Single Sign-on (SSO) via credentials provided by another Identity Provider (IDP) such as RealMe, Facebook, Google, Microsoft etc. Please specify methods available.	
AC12	Who creates the account/s in the third-party service?	
AC27	Do your support staff require remote access to end user devices?	
AC36	Are user accounts generated centrally, or by end users?	

Data Security

Protects sensitive information from unauthorized access, corruption, or theft throughout its lifecycle.

#	Questions	Standard/Controls
DS06	Who authorizes the transfer of data, including the data scope (e.g., student academic results) and scale (e.g., only year 8 students) from the service (data integration/aggregation service, data broker, data hub, data distribution hub) to recipient third party systems.	NIST 800-53 CA-3
DS17	For the service, is a separate, sandboxed execution domain maintained for each executing system process?	NIST 800-53 SC-39



Privacy

Ensures that personal data is collected, used, and protected in compliance with laws and regulations to safeguard individual privacy rights.

#	Questions	Standard/Controls
PR01	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.	
PRO2	Select the response option which best describes the publication of results on the service. Results are considered to be published if they are visible to anyone other than the owner of the results.	
PR03	What additional student data - other than that which is mandatory to register an account - can be provided to / collected by the service when used for its intended purpose? Please indicate whether this data field is mandatory or optional.	
PR05	What additional student, staff and/or parent data - other than that which is mandatory to register an account - can be provided to / collected by the service when used by the school for its intended purpose? This question is not intended to collect information about parent's personal use of the service (e.g., when it is not associated with school use/subscription). For each data asset, please specify whether it relates to student, staff, or parent. Select N/A if not collected.	
PR06	What, if any, other data not listed above can be disclosed to or collected by the service if used for its intended purpose? Please specify if data relates to student, staff or parent and whether it is mandatory or optional.	
PR13	Does the service provide any discovery functionality which allows users from one school to find, access or discover users or personal information from another school, or organization? 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.	
PR14	Does the service capture a user's location data?	
PR16	What mandatory information is collected by the service when school staff generate their own accounts for this service? Select all that apply. If not required, select N/A.	
PR17	What mandatory information is collected by the service when students generate their own accounts for this service? Select all that apply. If not required, select N/A.	
PR18	What mandatory information is collected by the service when parents generate their own accounts for this service? Select all that apply. If not required, select N/A. NOTE: This question relates to when parent accounts are required for school use of the service. If parent accounts are not required, select, 'N/A parent accounts are not required for school use of this service'.	

Privacy

Ensures that personal data is collected, used, and protected in compliance with laws and regulations to safeguard individual privacy rights.

#	Questions	Standard/Controls
PR19	What mandatory information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of school staff? Select all that apply. If not required, select N/A.	
PR20	What mandatory information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of students? Select all that apply. If not required, select N/A.	
PR21	What mandatory information is collected by the service when a school-based administrator (or the service) generates accounts on behalf of parents? Select all that apply. If not required, select N/A.	
PR22	Do the terms of use for the service require complete and accurate information to be entered when registering accounts for the service (e.g., are the use of pseudonyms or de-identified information not permitted)? Please include excerpt(s) from the terms of service. Are customers/users offered anonymity and/or pseudonymity when dealing with the service provider in some circumstances (e.g., providing feedback)?	
PR23	Are customers/users offered anonymity and/or pseudonymity when dealing with the service provider in some circumstances (e.g., providing feedback)?	
PR24	Are mandatory fields clearly distinguished from optional fields during the standard account registration process?	
PR25	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)?	
PR26	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?	

Safeguarding

Protects the welfare and safety of individuals, particularly vulnerable groups, within the organization or its influence.

#	Questions	Standard/Controls
SA01	Does the service contain, display, or promote the following via any means (social media or news feed, direct advertising, pop-ups): • Products/services: alcohol, controlled or banned substances, gambling, tobacco products, firearms and firearm clubs, adult products and pornography. • Categories of information which may be deemed offensive by a reasonable member of the school community (e.g., racist, sexist, pornographic content etc.)?	
SA02	When using the service, are users under the age of 18 exposed to advertising and/or offers?	
SA03	In relation to the commenting and communities/forums functionality available within the service, select all that apply.	
SA04	Who can publish content to content libraries within this service (i.e., users or service provider); and is content subject to moderation to ensure users are not exposed to information, including images, video, text and/or recordings, which may be deemed: • Offensive by a reasonable member of the school community (e.g., nudity, pornography, graphic content, profanity, racist, sexist etc. and/or • Inappropriate for users under 18 years? Moderation may include: • The service reserves the right to remove content that breaches the Terms of Use • The service applies a profanity filter • The service has an implemented assurance procedure to ensure content conforms to quality standards prior to publication • Users can report content that breaches the Terms of Use Select all that apply.	
SA05	In relation to the chat/instant messaging functionality available within the service, select all that apply.	NIST 800-171 3.1.12 NIST 800-171 3.13.12 NIST 800-171 3.13.14

•

Product Information

Provides detailed and accurate data about a product's features, usage, and benefits to consumers and stakeholders.

#	Questions	Standard/Controls
PI01	If customers can or are required to supply data to the service, what methods or mechanisms are available to support this?	
PI02	For which countries are you submitting a survey response?	
PI03	Vendor name	
PI04	Vendor ABN	
PI05	Vendor NZBN	
PI06	Vendor US corporate number CRN	
PI07	Vendor UK registration number	
PI08	Registered Australian address of vendor	
PI09	Registered New Zealand address of vendor	
PI10	Registered USA address of vendor	
PI11	Country in which the company is registered for Australian customers	
PI12	Country in which the company is registered for New Zealand customers	
PI13	Country in which the company is registered for USA customers	
PI14	For Australian customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	
PI15	For New Zealand customers: Preferred vendor contact name Preferred vendor contact email Preferred vendor contact phone number	
PI16	Name of service	
PI17	Is the service compliant with the WCAG 2.1 Accessibility guidelines as per https://www.w3.org/WAI/standards-guidelines/wcag/?	
PI18	Version of service: If no published version number, use date of version.	
PI19	Is the service free or paid?	
PI20	For paid services, URL of pricing page	
PI21	Do you warrant that you have the legal authority to submit this product or service for an ST4S assessment?	
PI22	URL of service for Australian customers	
PI23	URL of service for New Zealand customers	
PI24	URL of service for USA customers	

Product Information

Provides detailed and accurate data about a product's features, usage, and benefits to consumers and stakeholders.

#	Questions	Standard/Controls
PI25	URL of Terms of Service/use for Australian customers	
PI26	URL of Terms of Service/use for New Zealand customers	
PI27	URL of Terms of Service/use for USA customers	
PI28	Purpose of the service?	
PI29	In relation to the file download functionality available, select all files types that can be downloaded within the service.	
PI30	What names do you, as the service provider, give to the various modules available within the service?	
PI31	Enter the URL for the service's Privacy Policy or upload the Privacy Policy document	

Product Functionality

Describes the capabilities and features of a product that fulfill user needs and requirements.

#	Questions	Standard/Controls
PF01	Select the functionality available within the service. Select all that apply.	
PF02	In relation to the quiz, poll and flashcard functionality, select which features are offered within the service. Select all that apply	
PF03	When sending correspondence via the service on behalf of the school, how does the service send email communication to the school's recipients/audience? Select all that apply.	
PF04	In relation to the content libraries available within the service, select all that apply. Content may include	
PF05	In relation to the notification and alert functionality available within the service, select all that apply.	
PF06	In relation to the online learning activities, assessment and/or game functionality available within the service, select all that apply.	
PF07	In relation to any other functionality that is offered by the service, select all that apply.	
PF08	In relation to the assessment or collection of health and well-being information through functionality available within the service, select all that apply.	
PF09	In relation to the assessment or collection of health and well-being information through functionality available within the service, select all that apply.	
PF10	Select all functionality available within the service.	

Product Functionality

Describes the capabilities and features of a product that fulfill user needs and requirements.

#	Questions	Standard/Controls
PF11	In relation to the form, survey and/or eSignature functionality, select which features are offered within the service. Select all that apply.	
PF12	In relation to the online meeting, video conference, audio conferencing and/or livestreaming functionality available within the service, select all that apply.	NIST 800-171 3.1.12 NIST 800-171 3.13.12 NIST 800-171 3.13.14