

Global Education Security Standards (GESS) Overview

**We WANT
your input!**





Global Education Security Standard (GESS)

Steve Smith, Executive Director, Access 4 Learning

Connie Coy, Cybersecurity Analyst, MOREnet

Josh Olstad, IT Director, Oyster River Coop

Brian Rowse, Chief Information Officer, ParentSquare



Introductions

Steve Smith, Executive Director, Access 4 Learning

Connie Coy, Cybersecurity Analyst, MOREnet

Josh Olstad, IT Director, Oyster River Coop

Brian Rowse, Chief Information Officer, ParentSquare

Heightened awareness & attention paid to school cyber security - not so much on Edtech vendors' expectations



K12 Cybersecurity Resources

U.S. Cybersecurity
& Infrastructure
Security Agency



U.S. Office
of Educational
Technology



K12-Six Essential
Controls



MS-ISAC



COSN
Cybersecurity



NIST
Cybersecurity



Why Are We Here?



Seems like a lot
of resources
being devoted
to K12?

Lots of great work
going on to help
schools address
cybersecurity
locally

Where does the
majority of
students' data
reside today?



EdTech Providers

How are you all ensuring your students data is being properly secured by EdTech providers

According to the [Verizon Data Breach](#) report Ed Tech suffered 497 incidents with 238 with confirmed data disclosure. #? Breaches of student data held by EdTech providers last year

How are EdTech Providers meeting privacy obligations?

- Sign DPAs but how do we know they are following through?
- What controls are providers implementing to secure data?
- What standards do we hold them accountable to?

For EdTech Providers, how do they know what controls to implement?

Security Requirements to Meet Privacy Obligations

- No standard Requirement
- “Industry Standards”
- “Best Practices”
- Some Jurisdictions have mandated control sets; NH, NY, IL, TX, AU, NZ,
- Some have strict guidance; DfE (England)
- Most do not
- Everyone is struggling consumers & providers

District Perspectives

- Current frameworks
- Districts do not have the legal resources to ensure Edtech vendors are complying.
- Free apps
- GESS in DPAs
- Establishes common ground in agreement negotiations.
- Provides a crosswalk of controls/criteria focused on PK-20.
- Reputable standard frameworks



Vendor/Provider Perspectives

- Existing security frameworks don't cover K-12 topics
- Laws require/imply that schools should vet vendor security
- Schools request that vendors complete various questionnaires to cover K-12 topics
- Single set of controls with standardized assessment process would provide confidence to schools and streamline contracting



Wouldn't it be nice if....

There was an education sector agreed upon set of cybersecurity controls that;

- Worked across jurisdictions
 - Included a crosswalk to all current frameworks
 - Was adopted by all schools & EdTech providers
- Was publicly available
 - Could be assessed against
 - Could eventually have badges or certifications showing alignment?

Introducing...



GESS

Global Education Security Standard



Where to start...

Where to start on a Global Education Security Standard?

ST4S
Introduction

Leverage
the work
of ST4S

Mapping
ST4S and all
relevant
frameworks

Identify specific
controls across
frameworks
Format & publish
new set of
controls

What is ST4S?

An assessment framework for digital products and services used in the Australian & New Zealand Education Sectors against agreed criteria for:

Security

Privacy

**Functionality /
Online Safety**

Interoperability

Started with Australian States and Territories only, expanded recently to include New Zealand.

Sample report (front page)

Safer Technologies 4 Schools Assessment

Sample product/service (Sample vendor)

Assessment outcome: Medium risk

A non-compliant assessment outcome means the service does not meet the minimum requirements for information security, privacy, and/or online safety.



Service summary

Version:	Paid – Latest	Review date:	18/05/2020
Tags:	Library management; Administrative support services; Booking systems.	Assessment Tier:	Tier 2
URL:	http://www.sampleproduct.com.au	Audience:	Staff and Students
Purpose of use:	Sample product is a library management system. Modules include cataloguing, circulation, search, overdue notices, borrowers, reports and stocktake.		

Information assets and hosting

Data hosting:	Service components	Onshore (in Australia)	Data classification:	☒ Non-personally identifiable information
----------------------	--------------------	------------------------	-----------------------------	---

ST4S Observations

- Engaged with over 400 products/services
- Genuine, detailed assessments are hard and take time
- Just over 50% completion rate
- Most suppliers want to do the right thing
- Majority of suppliers make changes to improve their offerings

All suppliers appreciative of consistent approach with shared results

Global Education Security Standard

Establish a consolidated approach:

- Leverage shared efforts and success of SDPC (USA)
- Leverage assessment approach and success of ST4S (AU/NZ)

Geared to online products / services

Considers a number of existing frameworks:

- NIST 800-171 & 800-53
- CIS – Critical Security Controls v8
- UK Cyber Essentials (July 2022)
- AU ISM, NZ ISM

Draft set developed of control statements with assessment questions and possible answers

Global Education Security Standard (GESS)

Identify and document a security framework that could be a global security blueprint leveraging the ST4S work in the AU.



[Presentation shared with your 'SI'...](#)
[SDPC Community Update Aug 20...](#)
[Mappings - Google Drive](#)
[NIST 800-171 Matrix - Google Sh...](#)

[docs.google.com/spreadsheets/d/16oQTo655aivgr-wjMorTkuJ3RxeW84sZKPndSuR5Sa0/edit?gid=0](#)

NIST 800-171 Matrix

File Edit View Insert Format Data Tools Extensions Help *Last edit was made 19 days ago by Martin Rothbaum*

100% 11 Calibri

	A	B	C	D	E	F	G	H	I	J	
	NIST 800-171 Control	Control Type	Control Text		NIST 800-53	ST4S detail		UK Cyber Essentials	Valid in education SaaS context?	Applicability Scope	Suitability Notes/Use Cases
1	3.1.1	Basic	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).		AC-2, AC-3, AC-4	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?		User access control	Essential	Product	
2	3.1.2	Derived	Limit system access to the types of transactions and functions that authorized users are permitted to execute.		AC-2, AC-3, AC-4	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?		User access control	Essential	Product	
3	3.1.3	Derived	Control the flow of CUI in accordance with approved authorizations.		AC-4				Essential	Product	Will result in multiple controls being facing (firewalls and other bound packet inspection etc)
4	3.1.4	Derived	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.		AC-5				Essential	Both	Will require controls for the prod administrators vs end users and there separate testing teams vs d
5	3.1.5	Derived	Employ the principle of least privilege. Including for specific security functions and privileged accounts.		AC-6, AC-6(1), AC-6(2)	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)?		User access control	Essential	Product	
6	3.1.6	Derived	Use non-privileged accounts or roles when accessing nonsecurity functions.		AC-6(2)			User access control	Optional	Product	If product supports role based access advice regarding product configu
7	3.1.7	Derived	Prevent non-privileged users from exercising privileged functions and audit the execution of such functions in audit logs.		AC-6(9), AC-6(10)	A6-Are vendor staff, external contractors or associates with non-privileged accounts restricted from installing, uninstalling, disabling or making any changes to software and system configuration on servers and endpoints? 1.1- Does your organisation have a documented and implemented logging procedure which requires all systems in your organization (e.g., servers, storage, network, applications, etc.) to log the following and synchronise logs to a consistent time source:		User access control	Essential	Product	Requires at least 2 controls: RBAC logs

3.1 Access Control 3.2 Awareness Training 3.3 Audit & Accountability 3.4 Configuration Management 3.5 Identification & Authentication 3.6 Count: 2

GESS Examples

Multi-factor authentication

NIST 800-171: 3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

CIS 6.4: Require MFA for remote network access.

CIS 6.5: Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

AU ISM 1173: Multi-factor authentication is used to authenticate privileged users of systems.

NZ ISM 16.7: To ensure authentication systems incorporate Multi-Factor Authentication mechanisms to secure Privileged Accounts and in accordance with the Agency's Privileged Access Management (PAM) policy.

UK A7.14: Have you enabled multi-factor authentication (MFA) on all of your cloud services?

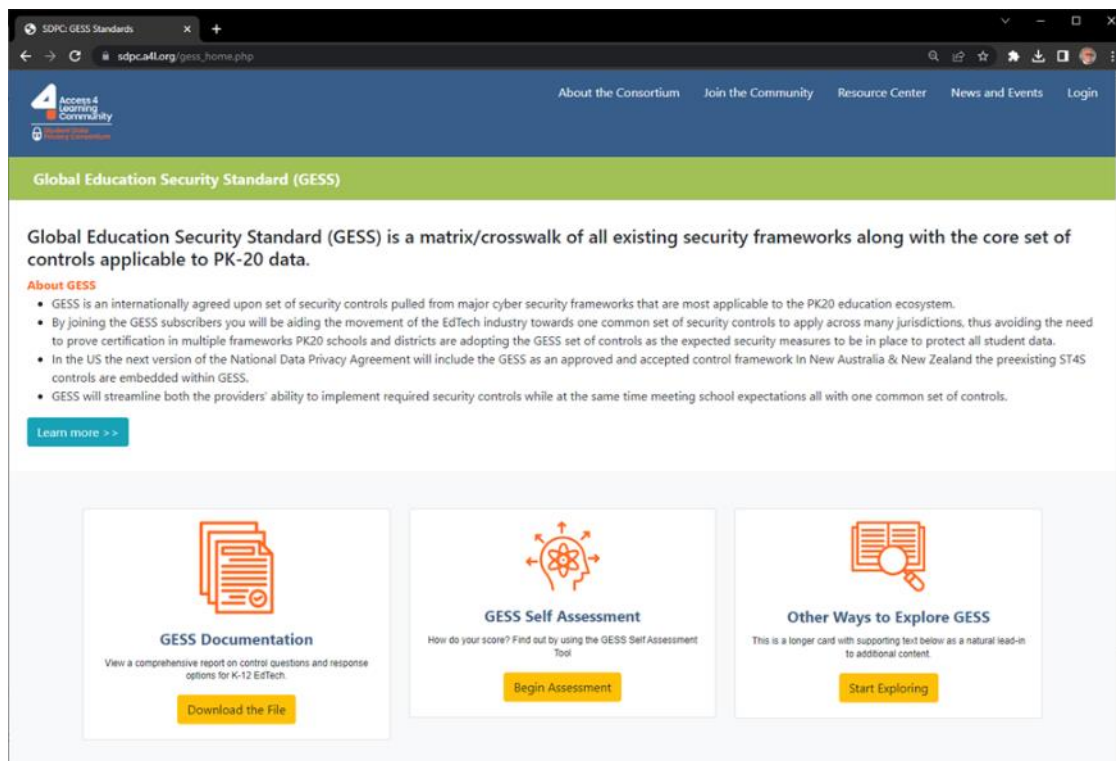
UK A7.16: Has MFA been applied to all administrators of your cloud services?

Announcement

GESS V1.0 Released 5/18/23



GESS Portal



The screenshot shows the GESS Portal website. The browser address bar displays 'sdpcall.org/geess_home.php'. The website has a blue header with the 'Access 4 Learning Community' logo and navigation links: 'About the Consortium', 'Join the Community', 'Resource Center', 'News and Events', and 'Login'. Below the header is a green banner with the text 'Global Education Security Standard (GESS)'. The main content area features a paragraph: '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.' This is followed by an 'About GESS' section with a bulleted list of points. Below the list is a 'Learn more >>' button. At the bottom, there are three white cards with orange icons: 'GESS Documentation' (document icon), 'GESS Self Assessment' (atom icon), and 'Other Ways to Explore GESS' (magnifying glass icon). Each card contains a brief description and a yellow button ('Download the File', 'Begin Assessment', and 'Start Exploring' respectively).

SDPC: GESS Standards

Access 4 Learning Community

Global Education Security Standard (GESS)

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.

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 next version of the National Data Privacy Agreement will include the GESS as an approved and accepted control framework In New 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.

[Learn more >>](#)

GESS Documentation

View a comprehensive report on control questions and response options for K-12 EdTech.

[Download the File](#)

GESS Self Assessment

How do your score? Find out by using the GESS Self Assessment Tool

[Begin Assessment](#)

Other Ways to Explore GESS

This is a longer card with supporting text below as a natural lead-in to additional content.

[Start Exploring](#)

GESS Self Assessment

Let's Get Started in 3 Easy Steps!



Step 1

Create a Vendor Account or Login to Your Account

Login

Create Account

Step 2

Complete the comprehensive product questionnaire.

Step 3

Take the Information Security Gap Assessment

Existing Users Login

OR

New Users: Create Account

Step 1

Create a Vendor Account or Login to Your Account

Login

Create Account

To login, complete the following information:

Submit

Step 1

Create a Vendor Account or Login to Your Account

Login

Create Account

To create an account, please complete the following information:

Save

New User Creates Vendor Account



-1- Complete Vendor Account

Please fill out the following to complete your vendor account:

Test Company
Select the country your company is associated with:
Australia
Vendor ABN
Registered Australian Address of Vendor
Country in which the company is registered for Australian customers
Preferred Vendor Contact Name
Preferred Vendor Contact Email
Preferred Vendor Contact Phone

Save

-2- Add Resources

Complete the comprehensive product questionnaire for each product.

-3- Your Ready!

Take the Information Security Gap Assessment

Vendor completes form for each resource.



**-1-
Complete Vendor
Account**
Your Vendor Account is
Complete



-2- Add Resources

Complete the comprehensive questionnaire below for each resource.

Resource Name

Product Name

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.)

- ☐ A. Yes (please specify)
- ☐ B. No (T2)

Is the service compliant with the [WCAG 2.1 Accessibility guidelines](#)?

- ☐ 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)

Version of service: If no published version number, use date of version.

Version

Is the service free or paid?

- ☐ A. Free
- ☐ B. Paid

Do you warrant that you have the legal authority to submit this product or service for an ST4S assessment?

- ☐ A. Yes
- ☐ B. No

URL of service for Australian customers

URL of Terms of Service/use for Australian customers

URL of service for New Zealand customers

URL of Terms of Service/use for Australian customers

URL of service for USA customers

-3- Your Ready!

Take the Information Security Gap Assessment

After New Vendor adds their resources, they are ready to start the assessment.

GESS Self Assessment

Welcome Lisa Waters from Lisa's Fake Company!



-1- Complete Vendor Account

Your Vendor Account is Complete



-2- Resources

Here is a list of all your resources:

Product 1
Product 2

[Add Another Resource >>](#)

-3- Your Ready!

Take the GESS Self-Assessment

[Begin >>](#)

Answering the Controls

Provide Feedback

Control Question

Relevant Controls

Choose Status

Upload Evidence

Add Notes

How to Take the Assessment

For each question, choose between **Fully Implemented**, **Partially Implemented**, or **Not Implemented**.

Your organisation have a current insurance policy of at least \$1M with claims for data breach/loss?

Relevant Controls: UKCE A3.1, UKCE A3.2, UKCE A3.3, UKCE A3.4,

Select One

☒ Fully Implemented
☐ Partially Implemented
☐ Not Implemented

Select All Resources

Upload Evidence (pdf)

Choose File No file chosen

Notes

Save and Continue >>

Provide Feedback
on this Control >>

Your Answers

Product 1
Partially Implemented
test

Product 2
Partially Implemented
test

View Previously
Submitted Answers

Select Resource(s)

GESS Self Assessment

Welcome Lisa Waters!



Return to Assessment and Filter By Status

How to Take the Assessment

For each question, choose between **Fully Implemented**, **Partially Implemented**, or **Not Implemented**.

You reached the end of the assessment. Here is the breakdown of your results for each resource:

Product 1

Fully Implemented = 0.00%

Partially Implemented = 0.96%

Not Implemented = 0.00%

[View Results >>](#)

Product 2

Fully Implemented = 0.00%

Partially Implemented = 0.96%

Not Implemented = 0.00%

[View Results >>](#)

View Detailed report

[Return to Assessment](#)

[Review Controls Marked Fully Implemented](#)

[Review Controls Marked Partially Implemented](#)

[Review Controls Marked Not Implemented](#)

[Review Missed Controls](#)

View Product Results By Status

Detailed Confidential Report Results

Product 2

Below is your confidential report results: ([Back to product listing >>](#))

Show 25 entries

Excel CSV Print Column visibility

Search:

	Control	Answer	Notes	Evidence
Change Answer	All relevant audit and logging data will be supplied to customers in response to customer requests.	Not Implemented	This is a test	Download
Change Answer	The organisation 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 organisation (e.g., servers, storage, network, applications, etc.) to log the following and synchronise logs to a consistent time source: - Authentication logs (e.g., successful login, unsuccessful login, logoff) - Privileged operations logs (e.g., access to logs, changes to configurations or policy, failed attempts to access data and resources) - User administration logs (e.g., addition/ removal of users, changes to accounts, password changes) - System logs (e.g., system shutdown/ restarts, application crashes and error messages) - And uses or ascribes a unique identifier of the user who has performed the activity being logged.	Fully Implemented		Download
Change Answer	The organisation has implemented a centralised 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.	Partially Implemented	Another test	Download
Change Answer	Your organisation have a current insurance policy of at least \$1M with claims for data breach/loss?	Partially Implemented	test	Download

Showing 1 to 4 of 4 entries

Previous

1

Next

GESS Next Steps/Roadmap

- Version 1.2 Released Feb 2024
 - Ensure CISA K12 Guidance Covered
- Included in National Data Privacy Agreement V2

- Continue Building vendor self assessment
- Accrediting cybersecurity auditors to assess and provide certifications
- Marketplace adoption



Global Education Security Standard

Q/A

**We WANT
your input!**

