Access 4 Learning Community

Simple. Secure. Scalable. Standard.

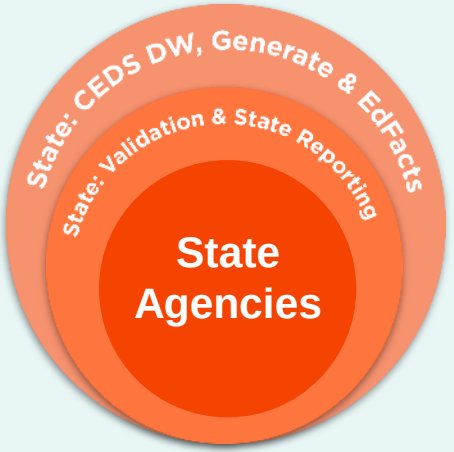
Global Education Security Standard (GESS) & Privacy Obligation Document (POD)

Steve Smith, Cambridge Public Schools
Connie Coy MOREnet
Jim Siegl, Future of Privacy Forum

Access 4 Learning Community

Simple. Secure. Scalable. Standard.

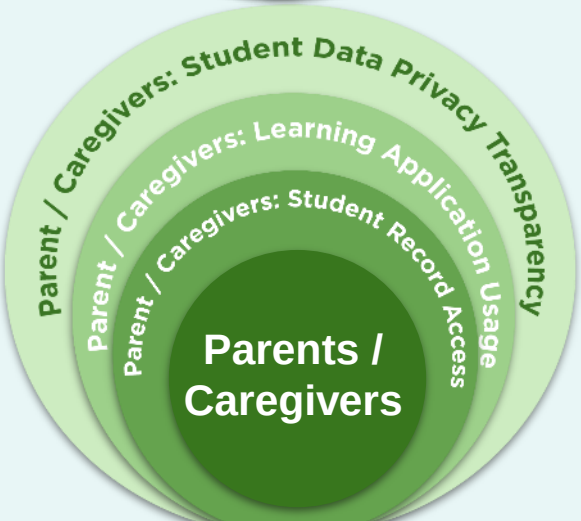
Increased interoperability without the inclusion of privacy requirements = increased RISK

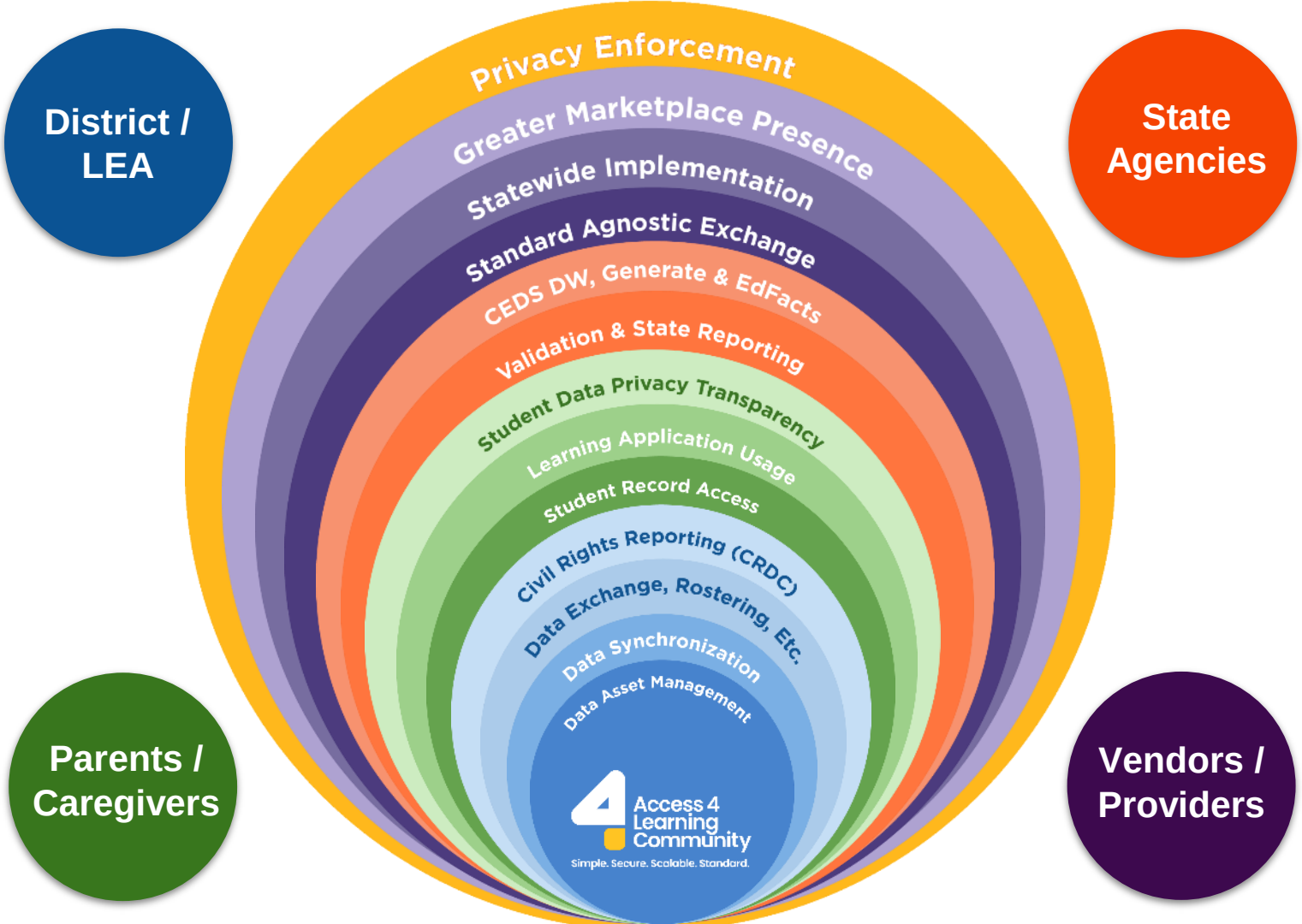


What's needed is a connected, secure, and effective learning ecosystem

Access 4 Learning Community
Simple. Secure. Scalable. Standard.

Access 4 Learning Community
Student Data Privacy Consortium





Connected and Secure Effective Learning Ecosystem™

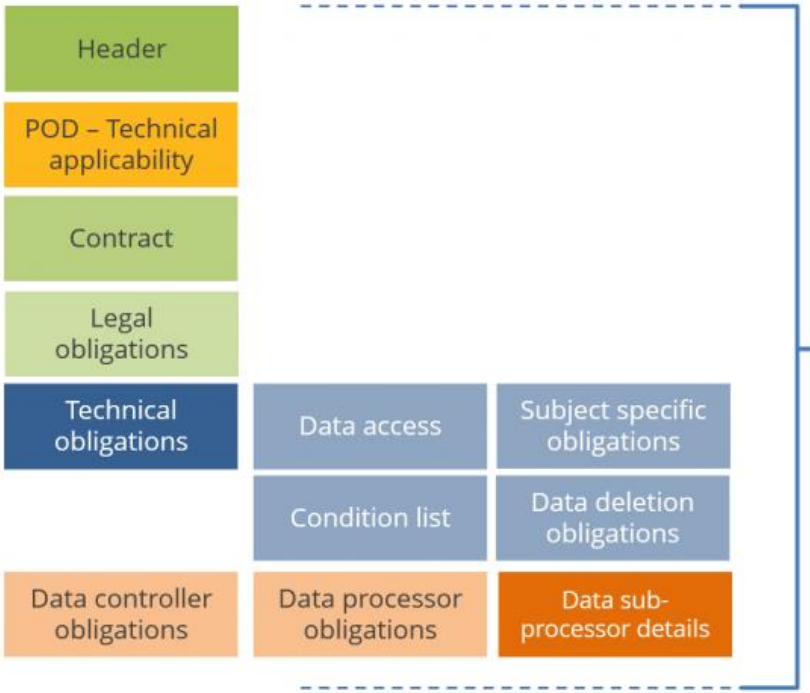
Access 4 Learning Community
Simple. Secure. Scalable. Standard.

Access 4 Learning Community
Student Data Privacy Consortium

It’s Not “One or the Other”!

“Connecting and Securing Effective Learning Ecosystems”®

Privacy Obligation Document

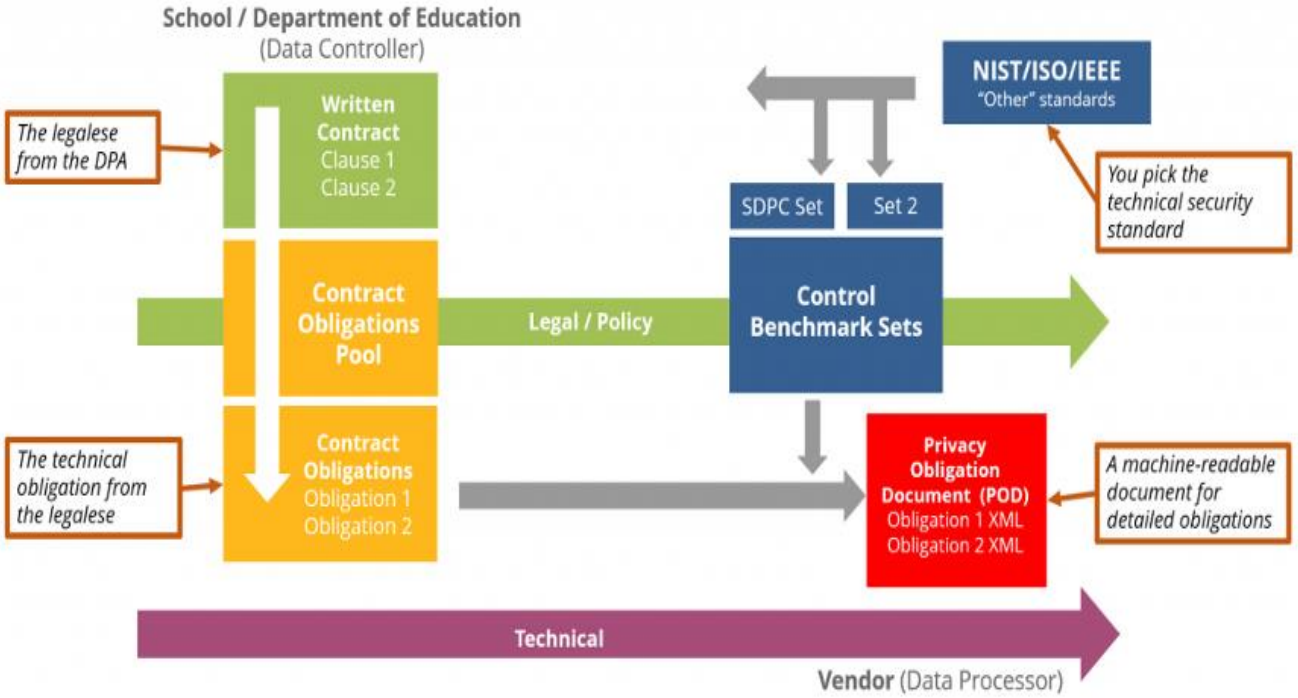


UNITY

Automate Contract Clause Expectations Exchange and Vendor Verification

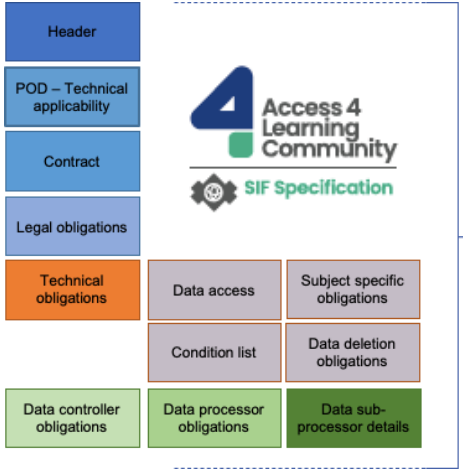
The "POD"
(Privacy Obligation Document)

End-to-End Privacy Solution?

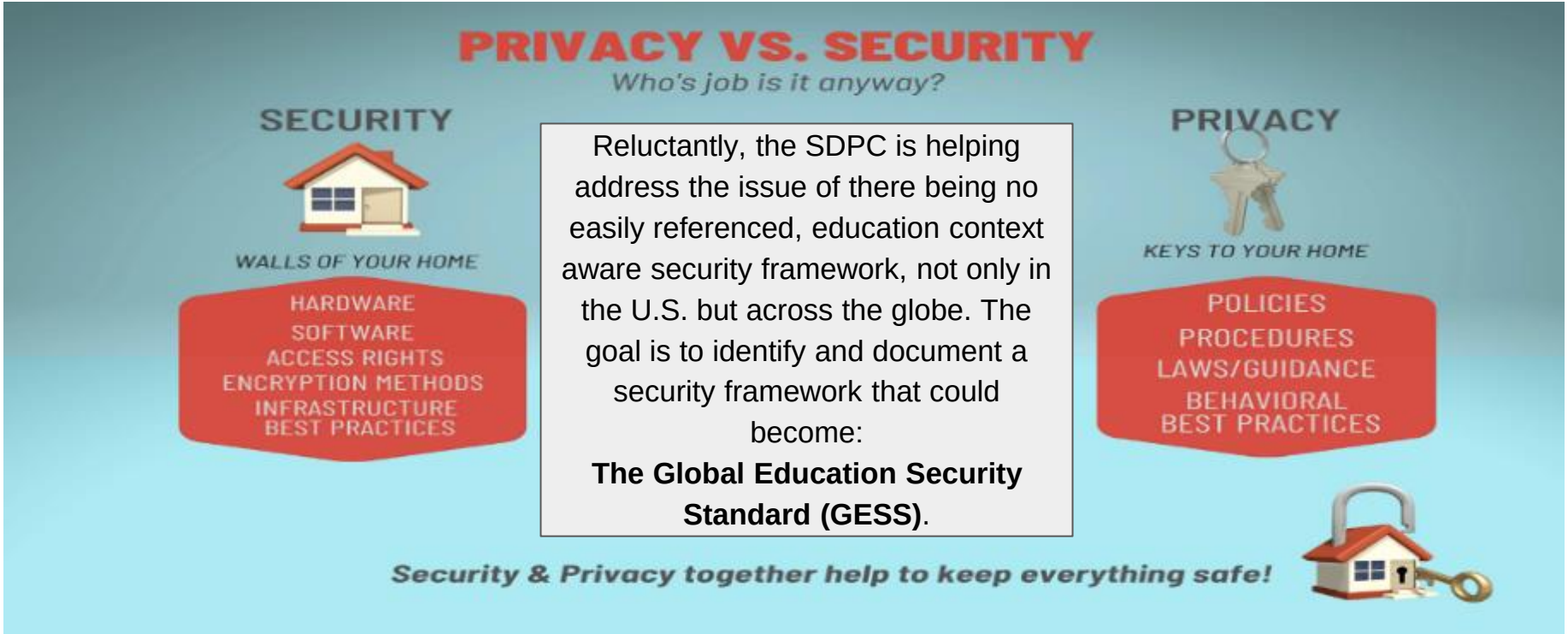


Automate Contract Clause Expectations Exchange and Vendor Verification

The "POD"
(Privacy Obligation Document)



Global Education Security Standard



Graphic from CITE: studentdataprivacy.net

Access 4 Learning Community
Simple. Secure. Scalable. Standard.

Security Requirements to Meet Privacy Obligations

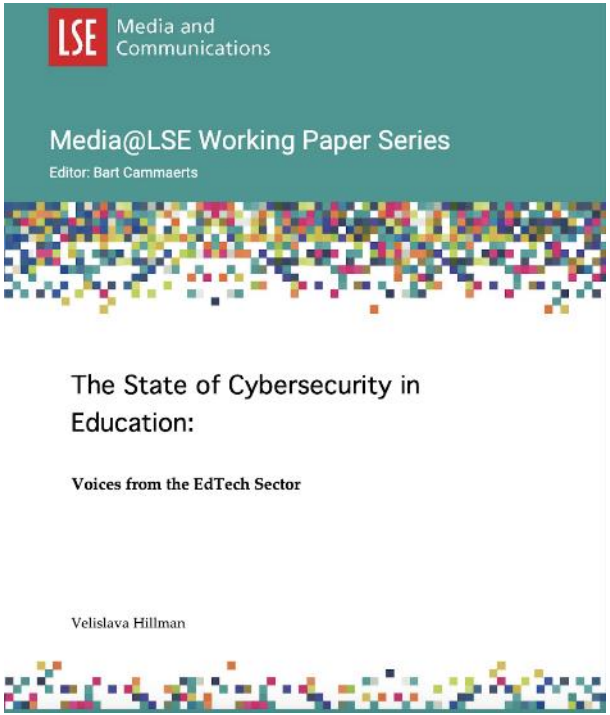
- No standard Requirement
- “Industry Standards”
- “Best Practices”
- Some Jurisdictions have mandated control sets; NH, NY, IL, TX AU NZ
- Most do not
- Everyone is struggling consumers & providers

Access 4 Learning Community
Student Data Privacy Consortium

District Perspectives

- Lack of providers understanding K-20 cybersecurity educational needs/concerns
- Provider's policies are not written to address district concerns.
- Provider Contract/District Agreements
- Free apps/free version
- Remove negativity from negotiations
- Reputable standard framework

An ideal cybersecurity standard must **underpin children's safety and data privacy** and **address the challenges** of the entire EdTech sector



CONNECT
Velislava Hillman (PhD)
veli@edds-education.org
EDDS @ ETOILE PARTNERS

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

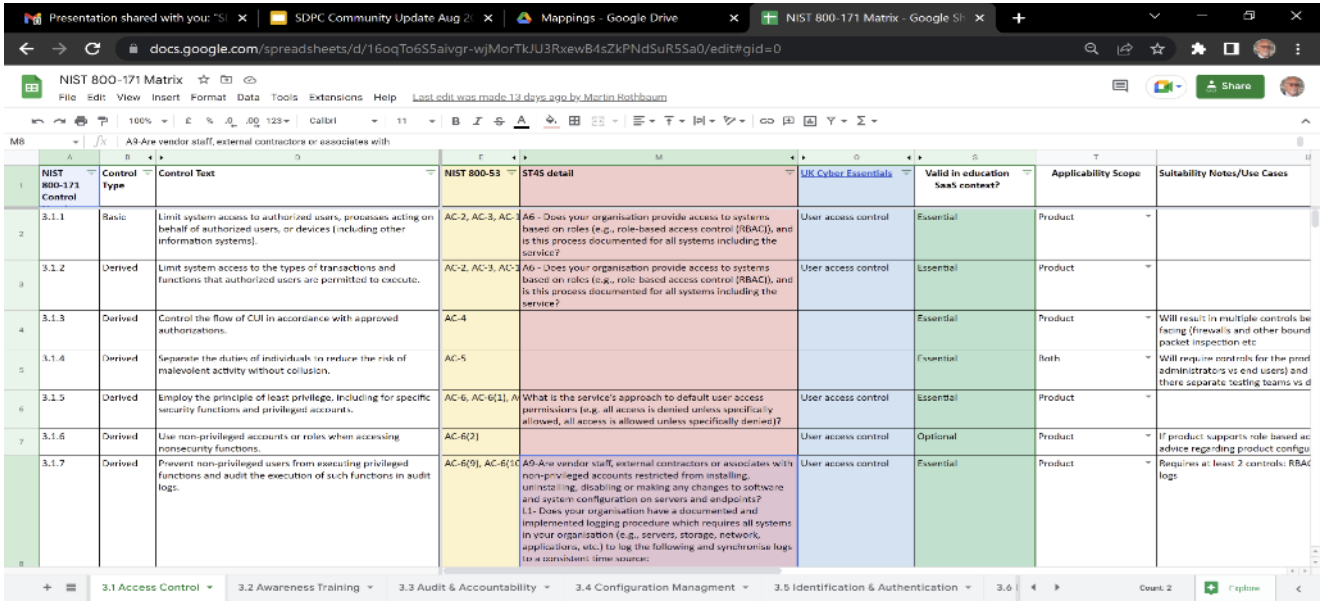
Considers a number of existing frameworks:

- 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.



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?

GESS Examples

Multi-factor authentication

Question format: Does your organisation mandate multi-factor authentication for:

Vendor staff, external contractors or associates accessing systems remotely (including access to cloud systems);

System administrators;

Support staff;

Staff with privileged accounts?

Control statement format: Multi-factor authentication is mandated for:

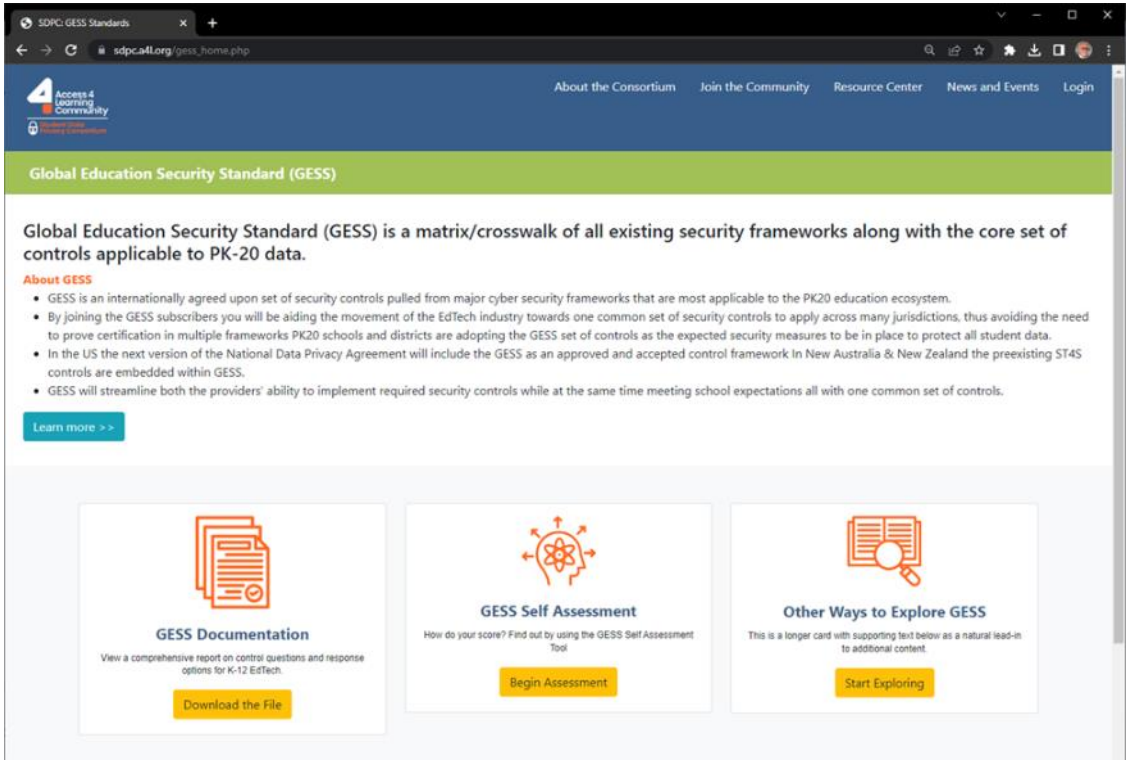
Vendor staff, external contractors or associates accessing systems remotely (including access to cloud systems);

System administrators;

Support staff; and

Staff with privileged accounts

GESS Portal


SDPC: GESS Standards
sdpc.a4l.org/gess_home.php
About the Consortium
Join the Community
Resource Center
News and Events
Login
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

ANNOUNCEMENT

GESS V1.0 RELEASED YESTERDAY!