Global Education Security Standards (GESS) Overview

We WANT your input!

Access 4 Learning Community & PESC

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

Access 4 Learning Community & PESC

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

Access 4 Learning Community & PESC

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

Access 4 Learning Community & PESC

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

Access 4 Learning Community & PESC

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?

Access 4 Learning Community & PESC

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….

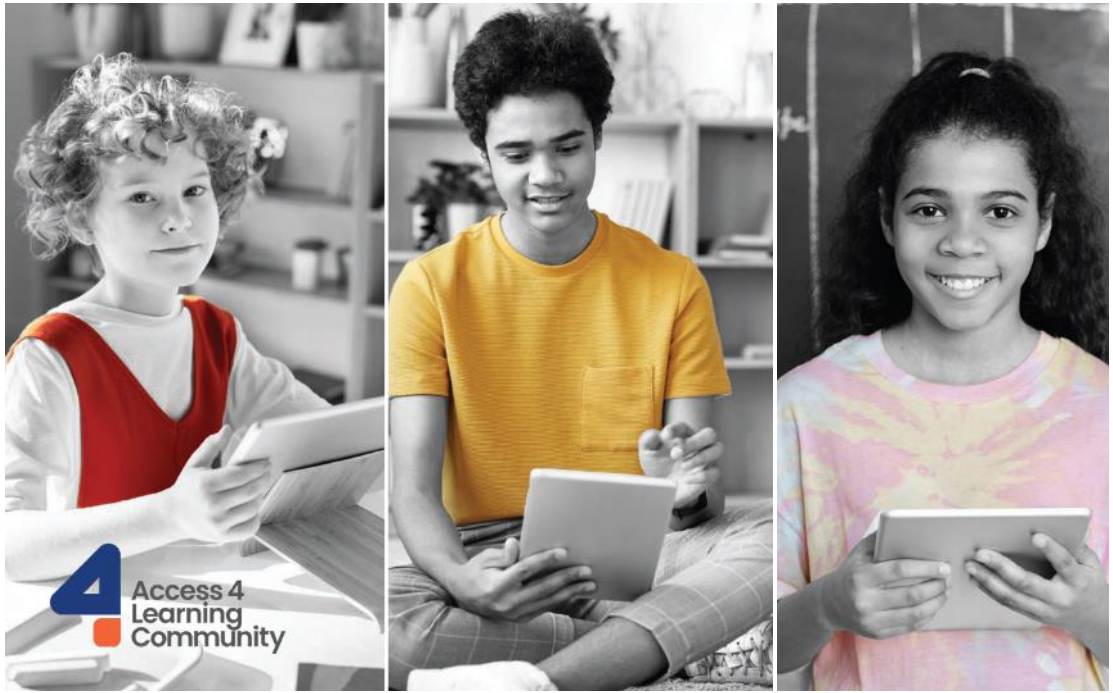
There was an education sector agreed upon set of cybersecurity controls that;

- 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



Access 4 Learning Community & PESC

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.

Access 4 Learning Community & PESC

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

Access 4 Learning Community & PESC

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

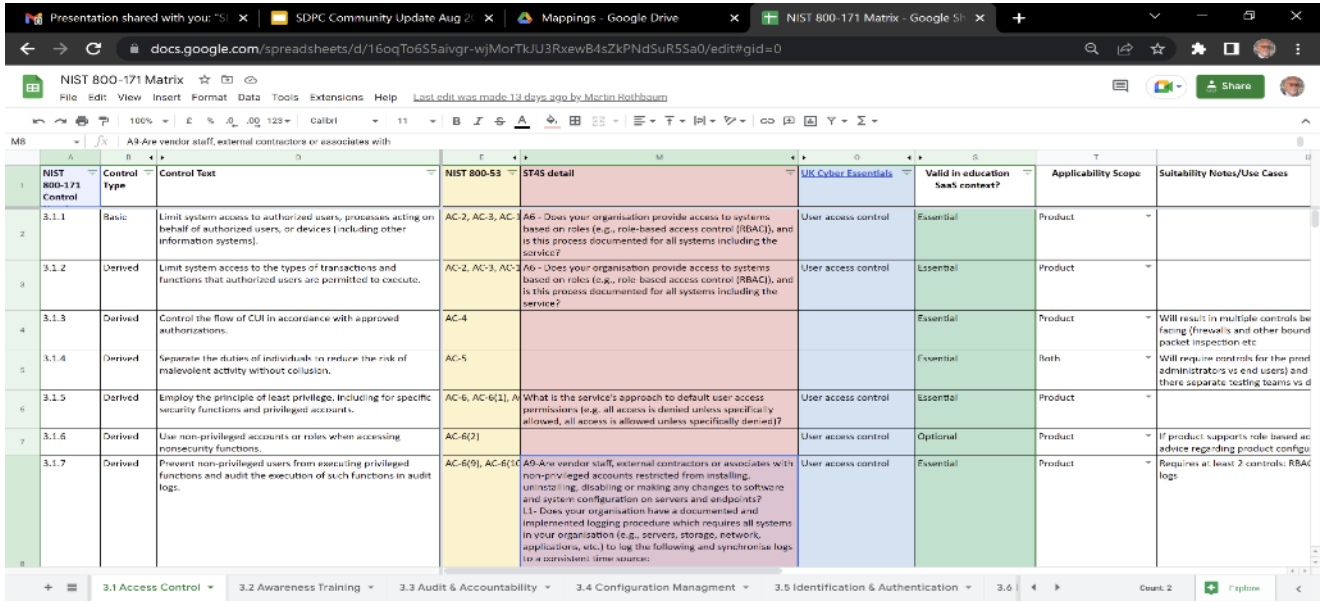
Considers a number of existing frameworks:

- 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.



Access 4 Learning Community & PESC

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?

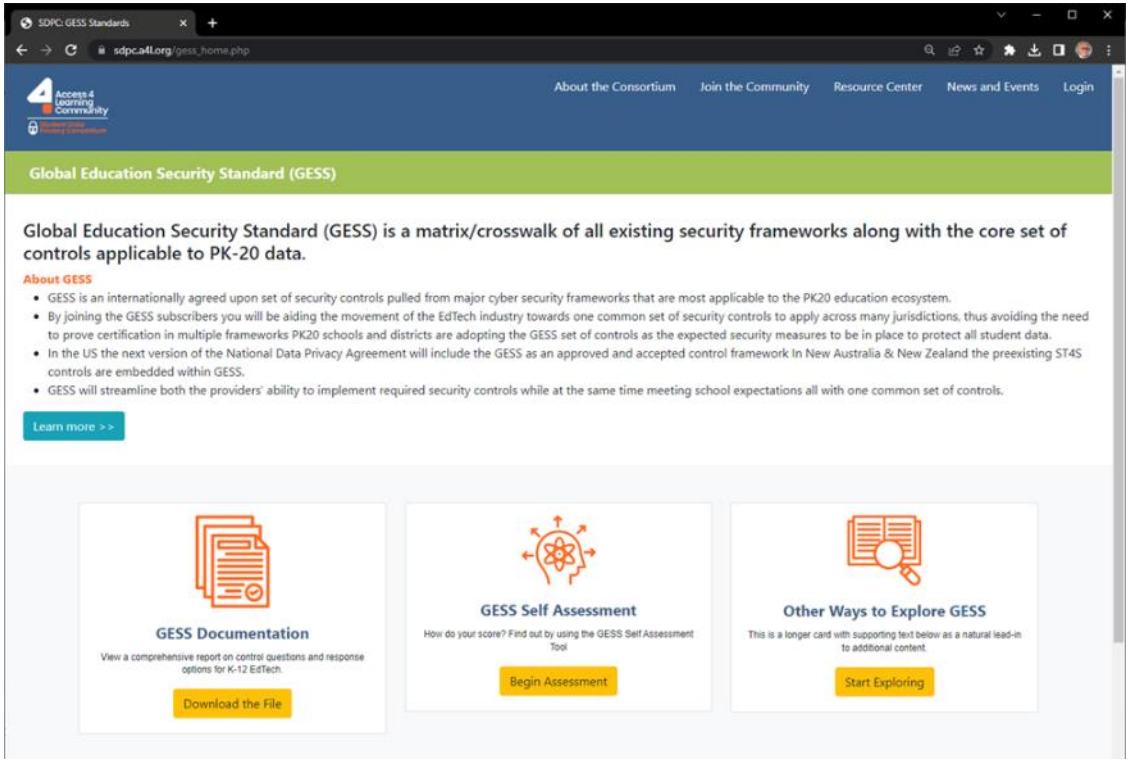
UK A7.16: Has MFA been applied to all administrators of your cloud services?

Announcement

GESS V1.0 Released 5/18/23

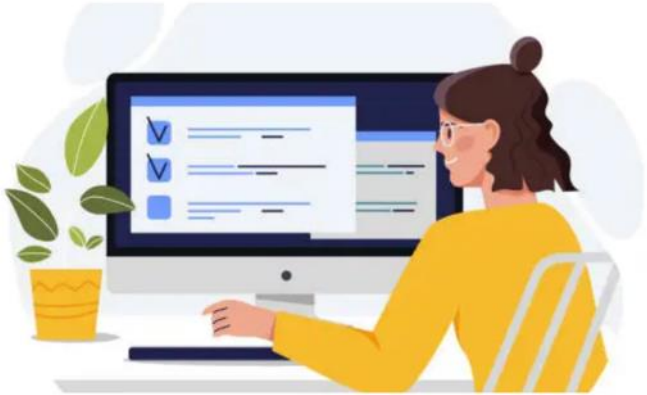
Access 4 Learning Community & PESC

GESS Portal



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.

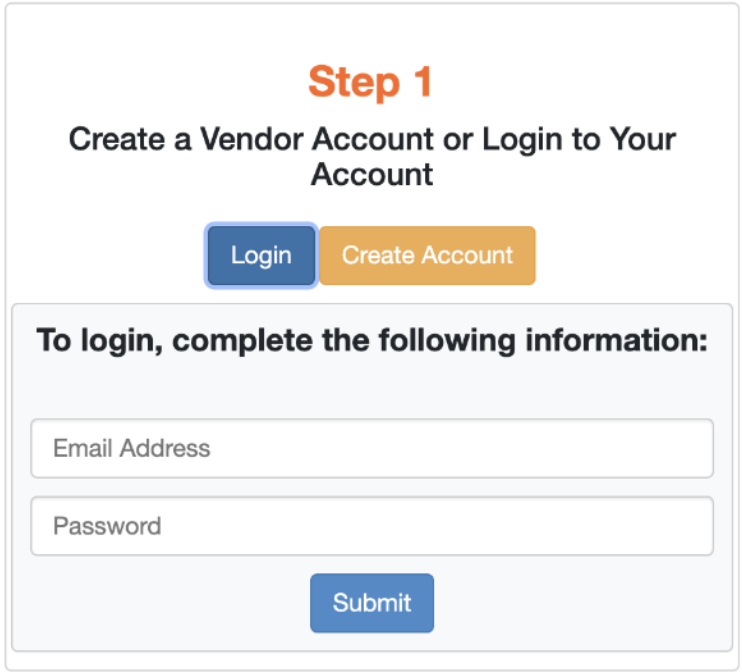
Step 3

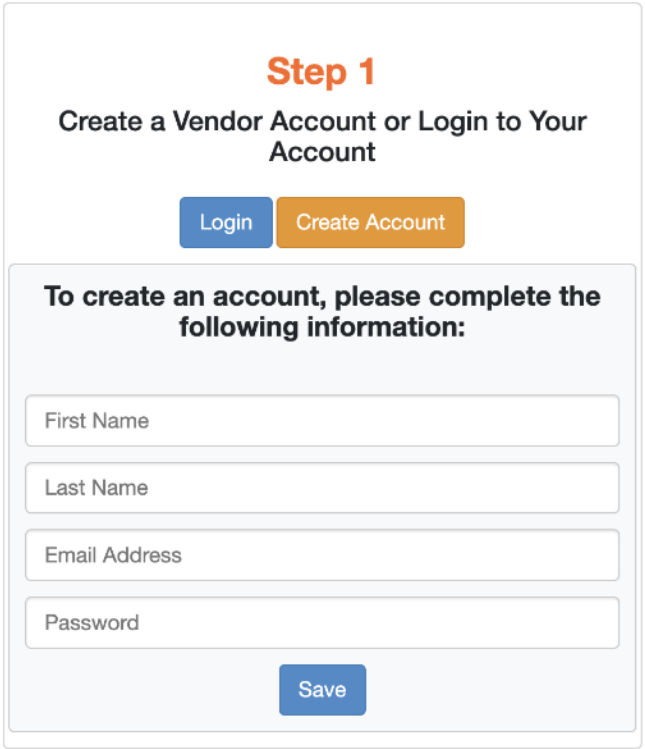
Take the Information Security Gap Assessment

Existing Users Login

OR

New Users: Create Account





Access 4 Learning Community & PESC

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

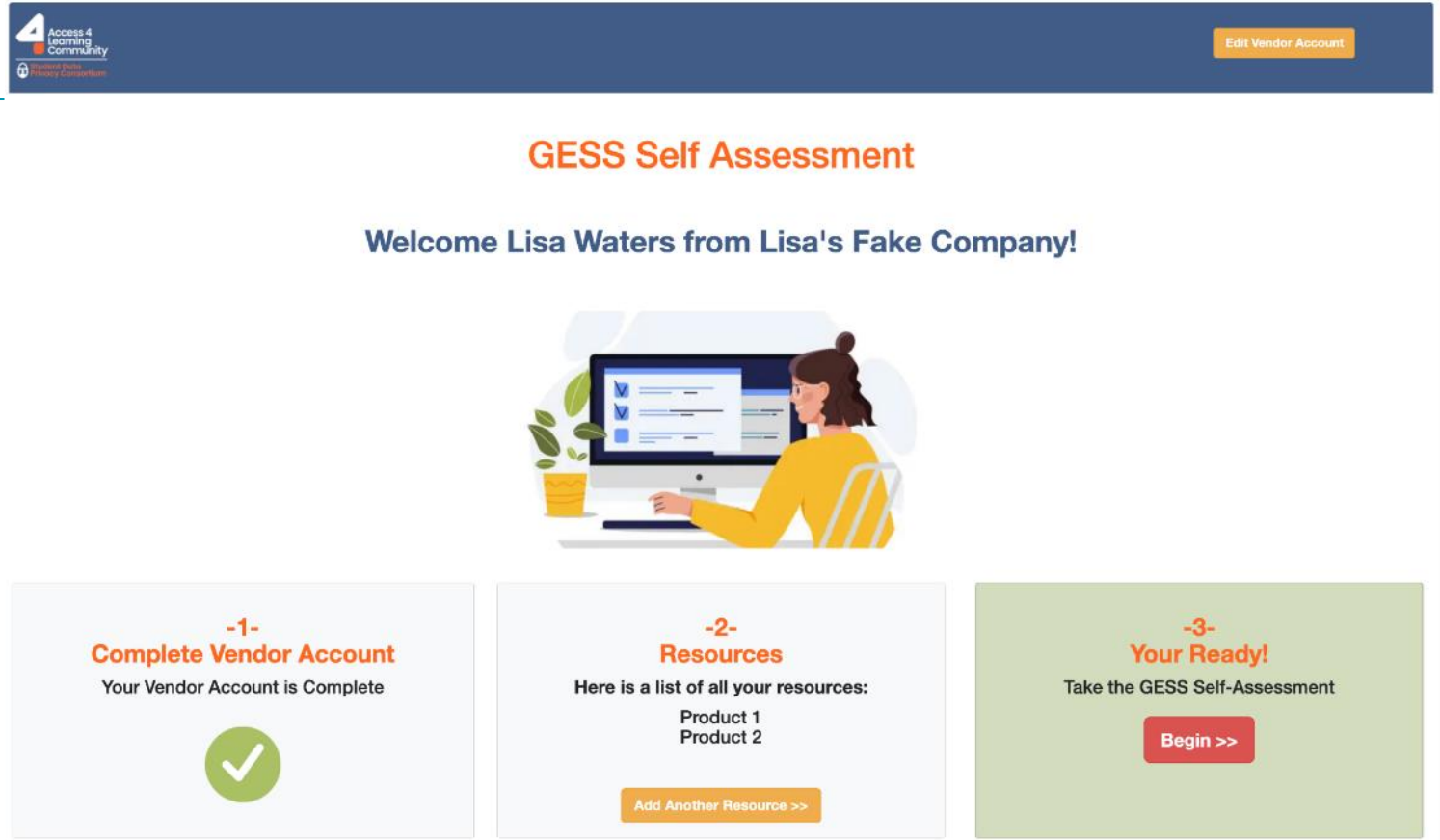
URL of service for USA customers

-3-
Your Ready!

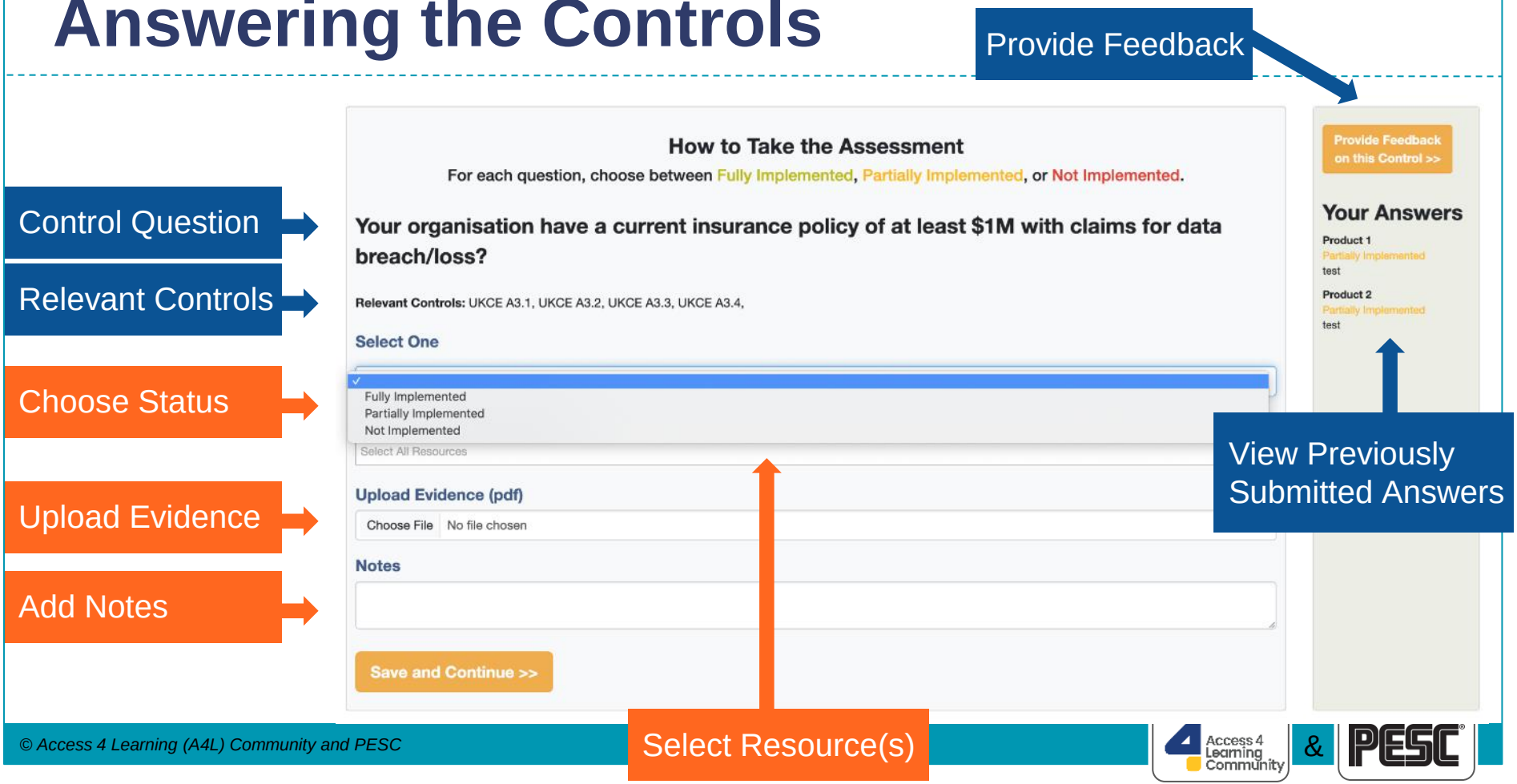
Take the Information Security Gap Assessment

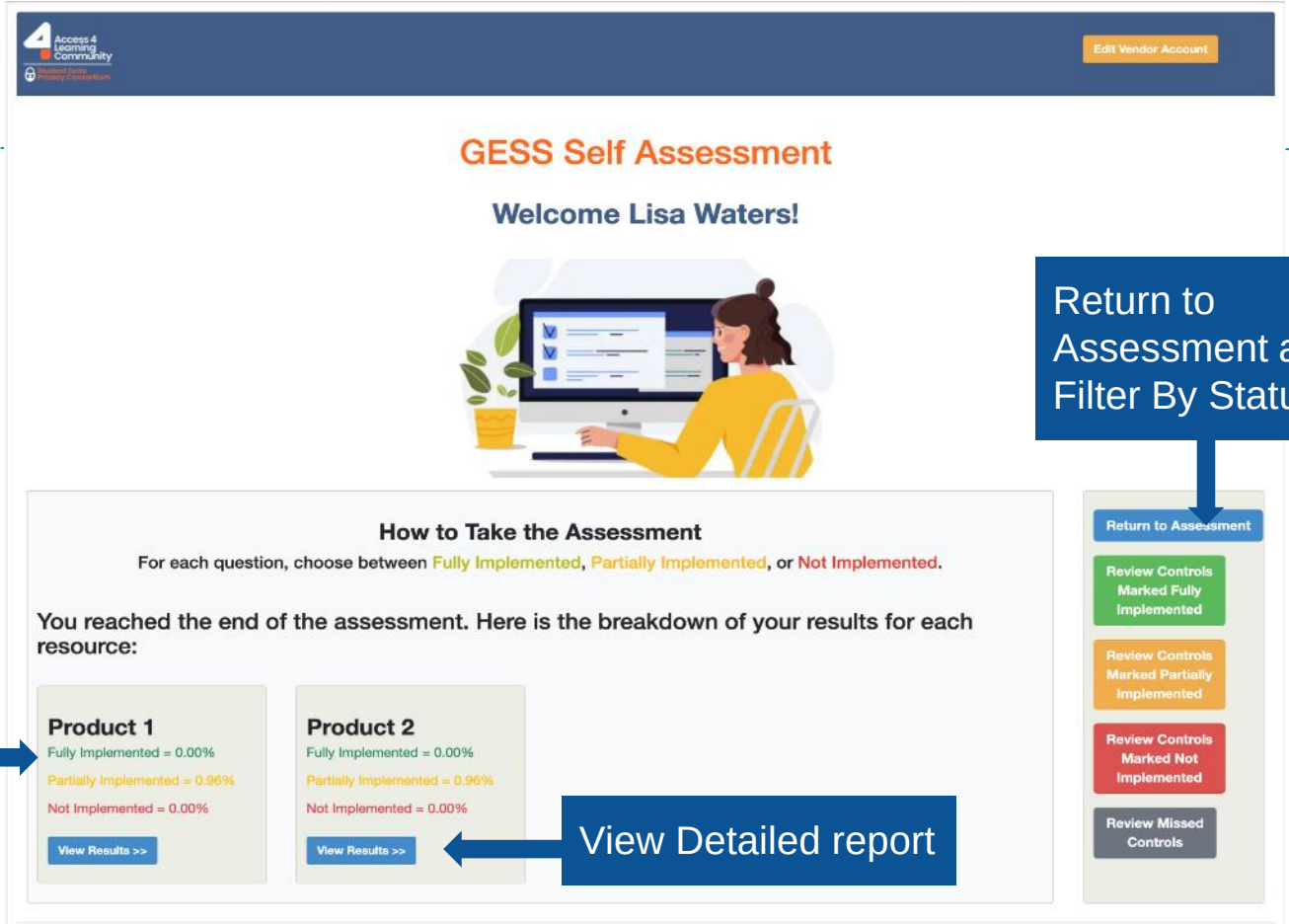
Access 4 Learning Community & PESC

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



Answering the Controls



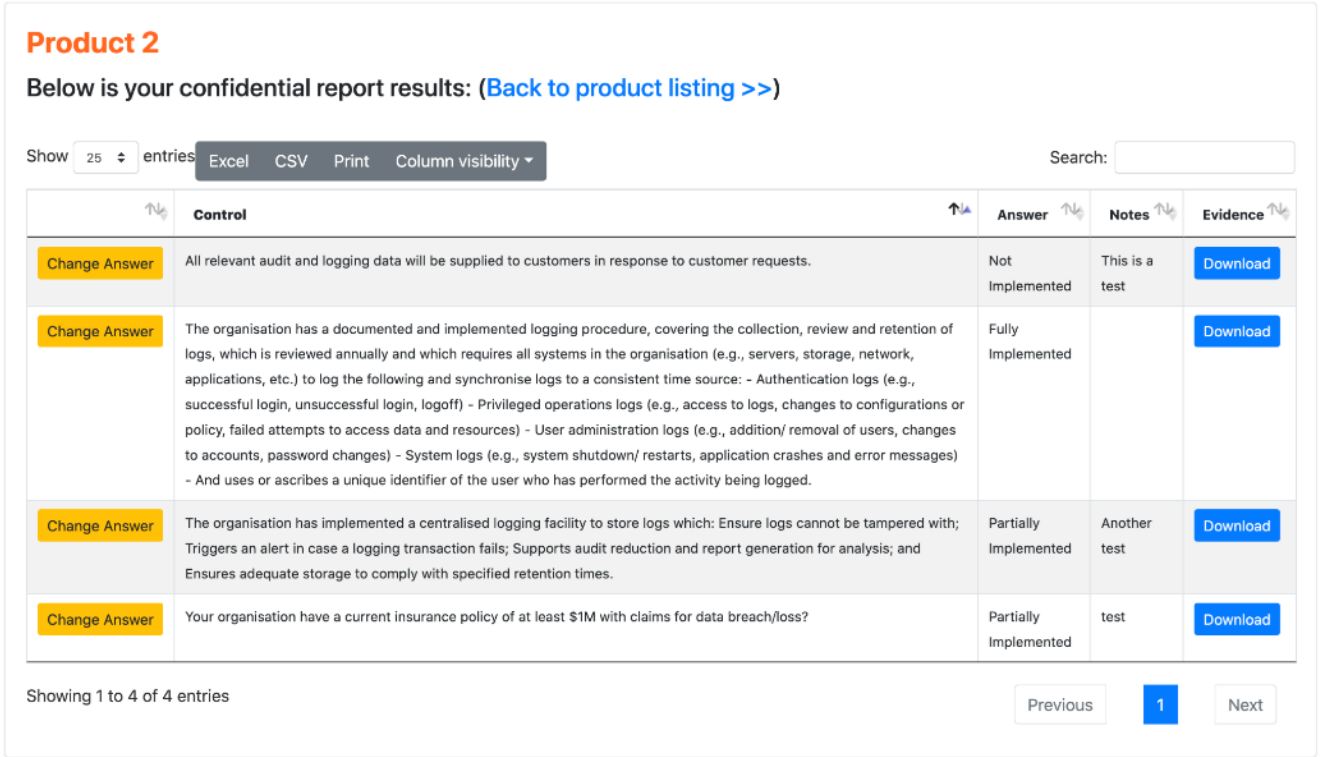


Return to Assessment and Filter By Status

View Product Results By Status

View Detailed report

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

Access 4 Learning Community & PESC

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!

Access 4 Learning Community & PESC