

REQUEST FOR PROPOSAL

The A4L Community is seeking proposals to develop an assessment framework for third-party certification to the Global Educational Security Standard (GESS) and to conduct assessments of K–12 educational technology products

Purpose of this RFP

This Request for Proposal (RFP) seeks to identify qualified, objective third-party cybersecurity firms to develop and conduct assessments for the A4L Community's Global Educational Security Standard (GESS) certification program. This program is intended to support K–20 educational technology providers in demonstrating their cybersecurity posture on a product-by-product basis through a standardized, affordable certification process. Ultimately, the goal of the certification is to increase trust in edtech products, reduce the burden on school districts to vet edtech apps, and improve the marketability of products that take the protection of student data seriously.

1. Overview

In late 2025/early 2026, the [Access 4 Learning Community \(A4L\)](#) plans to offer third-party certifications for its Global Educational Security Standard (GESS). We are currently seeking proposals from firms experienced in information security assessments or specialized in objectively auditing and certifying products for their compliance with cybersecurity frameworks to develop the third-party assessment framework for GESS and to conduct the assessments for educational technology provider companies of varying sizes, ranging from small startups to larger, more established companies.

For clarification, the scope of this RFP does not include assessing A4L or K–12 schools or districts directly.

1.1. Contact information

We have designated the following individual as the official point of contact for this RFP:

David Sallay, Director of Data Privacy

dsallay@a4l.org

(508) 202-0855

1.2. Questions

Please submit your responses to or questions about this RFP via email to the RFP point of contact before the RFP closure deadline identified in Section 1.3. A4L may share the responses to questions with other bidders in order to ensure that all firms intending to bid have access to the same information.

1.3. Timeline

- **August 26, 2025:** RFP opens
- **Sept 26, 2025:** Information call
- **October 31, 2025:** RFP closes
- **November 30, 2025:** A4L concludes reviews/Contract awarded (approximately one month for review)
- **December through Early 2026:** Formal development of assessment framework (we estimate 1 to 3 months depending on how much the firm will be able to leverage existing work)
- **Early 2026:** Publish availability of GESS third party assessments to edtech providers
- **Throughout 2026-2027:** Conduct GESS assessments as purchased by edtech providers

All of these dates are approximate, and A4L reserves the right, at its sole discretion, to modify them as needed.

1.4. RFP amendment and cancellation

A4L reserves the right to amend or cancel this RFP at its sole discretion. Any amendments will be published on A4L's website and shared with any firms who inform A4L of an intent to bid or opt into updates on the RFP.

1.5. Proposal submission

All proposals should be submitted via email to dsallay@a4l.org by 11:59pm ET on the RFP deadline date identified in section 1.2. Please clearly label your subject line with this format: **GESS RFP from [insert your firm's name]**

2. Background

2.1. Background on A4L

Started in 1997 by software providers and schools collaborating, the SIF Association – now the Access 4 Learning Community (A4L) – is a unique, non-profit collaboration composed of more than 3,000 schools, districts, local authorities, states, US and International Ministries of Education, software providers and consultants who collectively address all aspects of information management and access to support learning (more information on our membership and what is required to become a member can be found [here](#)). Specifically, A4L [maintains a data standard \(SIF\)](#) and also runs the Student Data Privacy Consortium (SDPC), which consists of a [National Data Privacy Agreement \(NDPA\)](#) and a [Resource Registry](#) of software providers that have agreed to the terms of the NDPA for their educational technology products (edtech).

A4L members may participate in several project teams, which are detailed [here](#). The Global Education Security Standard (GESS) project team is housed under the International Technical & Privacy Leadership Group and consists of volunteer representatives working in ministries of education in Australia and New

Zealand, state education agencies and regional service centers in the United States, and educational technology providers.

2.2. Background on educational technology providers

Educational technology is a multibillion dollar industry consisting of companies ranging from some of the largest tech companies in the world to small startups. When it comes to cybersecurity, their capabilities—and the ability to demonstrate those capabilities—varies just as much. Many smaller companies do not have adequate funding to complete security assessments like FedRAMP or SOC2. Furthermore, some educational technology providers have opted not to pursue these assessments since the data they hold on students is relatively low risk. Nevertheless, since education is a sector that is also regularly subjected to cyber attacks and threats, there is a growing need for a standardized, rigorous, yet cost-effective way for educational technology providers to demonstrate their security posture to schools.

2.3. Background on GESS

To address growing cybersecurity concerns from our members, in August 2024 A4L released its [Global Educational Security Standards \(GESS\)](#), which is a [matrix/crosswalk](#) of existing cybersecurity frameworks commonly used in the K–12 education sector, including the NIST CSF and CIS Controls and cybersecurity standards established in [Australia](#), [New Zealand](#), and the [United Kingdom](#), along with the core set of controls applicable to educational data contexts ranging from pre-kindergarten to higher education (collectively referred to as PK–20 data). As of right now, this has only been available to edtech providers as part of a self-assessment. A4L would like to expand this to a certification program wherein the edtech provider would receive a third-party assessment of their cybersecurity posture and receive a badge certifying their adherence to GESS should they meet all of the requirements.

In February 2025, A4L released a [Request for Information](#) to better understand what capabilities cybersecurity firms already have. Based on the responses we received, we are now releasing this Request for Proposals (RFP), which we anticipate will lead to awarding a contract to conduct the scope of work described herein.

3. Scope of work

3.1. Work with A4L to develop an assessment framework for the Global Educational Security Standards (GESS)

We are looking for a partner that will be able to take the existing GESS framework and develop an assessment framework that will be an attractive option for educational technology providers of all sizes. Specifically, we are looking for a framework that will meet the following parameters:

- Assessment framework needs to balance rigor and cost in a way that will allow for small edtech providers with smaller budgets to participate.
- Larger edtech providers getting other certifications (e.g., SOC2) should be able to count/leverage the findings from those assessments into getting a GESS certification, provided that they receive an appropriate assessment for any controls not covered under that certification.

- The framework should consider how to leverage and build upon the existing GESS self-assessment.
- The framework should include multiple tiers based on the edtech provider's size and the risks associated with the data they maintain.
- Assessments need to be conducted on a product-by-product basis (not enterprise-level), but ideally will be streamlined in a way that an edtech provider will not have to repeat the exact same process for each new product assessed.
- The proposal should include estimates for how long each phase of a complete assessment will take and include a description of the staffing needed.
- The assessment should provide for a remediation window that includes a plan of action for edtech providers that do not initially meet all of the requirements for certification.
- The assessment provider should provide detailed documentation that can be shared with the edtech provider but that also could be shared within the K–12 education community. In this way, once an edtech provider receives an assessment, that assessment should be valid and reviewable by all schools in the United States, United Kingdom, Australia, or New Zealand within the certification period.
- The framework should include timelines for validity and recertification based on the assessment tier and address how the edtech provider experiencing a data breach will impact their certification.

We anticipate awarding the development of the assessment framework to only one firm. Assets developed in support of the above activities will be the property of the Access 4 Learning Community and may be used by A4L to support audits conducted by additional cybersecurity firms.

3.2. Conduct assessments of edtech providers

Depending on demand, we anticipate awarding the ability to conduct GESS assessments to multiple firms. Once the framework is established, we anticipate publicizing the availability of third-party GESS assessments to the A4L edtech vendor member community as well as broadly to nonmember edtech providers. Upon receiving payment for an assessment from an edtech provider, we will contact the cybersecurity firm to initiate the assessment. We expect these assessments to be conducted within the timeline, budget, and other parameters established within the approved framework. Firms should be flexible enough to pivot to potential updates to the framework.

Unless agreed upon in advance by A4L and the assessed edtech provider, all data and information from the assessment will remain the property of the assessed edtech provider, and the assessing firm must destroy all information at the end of the assessment and may not use the data for any secondary uses not described in this scope.

4. Budget

A4L anticipates a program wherein A4L would enter a partnership agreement with the firm or firms to conduct the third-party GESS assessments. Individual edtech providers would then pay A4L for their participation in

the certification program. These funds will then be disbursed to the selected third-party cybersecurity firm, in accordance with an agreed upon revenue sharing agreement, to conduct the assessment.

5. Evaluation and Award

5.1. General information

The award will be made to the firm(s) offering an advantageous proposal to the services described in the scope of work. A4L shall not be obligated to accept the lowest priced proposal, but will make an award in its best interest and the best interest of its members. All proposals received in response to this RFP will receive a fair and impartial evaluation by A4L.

5.2. Requested information

Proposals should provide straightforward, concise answers that directly speak to the requested information. Marketing brochures and slide decks that do not directly provide the information requested below should not be included. We request that each submitted proposal minimally include the following components:

5.2.1. Cover letter

Each proposal should include a cover letter, which includes the following information:

- Proposer's legal name and corporate structure, including state incorporated in.
- Proposer's primary contact, including name, title, address, phone, and email.
- Identification of any subcontractors (if any) you anticipate would be used to conduct the scope of work.
- Statement indicating that any prices quoted are valid for at least 120 days.
- Statement that the proposer and anyone conducting work for the proposer is free of any conflicts of interest (e.g., employment at a school, district, or at an educational technology provider).
- Signature of a company officer empowered to bind the proposer to the provisions in the RFP.

5.2.2. Executive summary

Please include a brief synopsis of your firm's credentials and a description of how you intend to provide the services described in the scope of work. This section should be no longer than two (2) pages.

5.2.3. Company background and qualifications

Your submission should include sufficient details to demonstrate that you will be able to successfully and cost effectively conduct the GESS audits described in the scope of work. For this, you may include samples of prior work completed, proof of technical skills (e.g., certifications), descriptions of successful engagements with similar organizations, as well as references. Whereas it is not a

requirement that your firm have experience auditing educational technology providers, being able to demonstrate that you have experience auditing technology companies of a similar size and risk level will be looked on favorably.

5.2.4. Assessment framework proposal

The proposal should include a high-level framework for conducting assessments consistent with the requirements described in 3.1. In addition, you should explain your general approach to conducting cybersecurity assessments or audits and identify any assumptions, constraints, or risks to your approach.

5.2.5. Providing assessments

The proposal should include a description for how you plan to develop and execute a framework that meets the requirements described in the scope of work in section 3. This should include:

- a description of personnel who will be involved and the roles they will play
- a description any products or services you already have available to deploy versus ones you would have to develop
- an estimate of the expected turnaround time for assessments once initiated
- how many assessments your organization would be able to conduct in a year

5.2.6. Pricing

The proposal must include pricing for the services described. These should clearly balance cost versus rigor and be at an attractive price point for smaller educational technology software providers. Identifying cost-effective alternatives and other options, including an analysis of their strengths, weakness, and limitations, would also be appropriate.

5.3. Proposal scoring

Proposals will be evaluated by A4L's Global Education Security Standard project team, which will assess each proposal based on the following criteria. The percentages shown reflect how much each component will be weighed in the evaluation.

- 1. Proposal for how your organization would develop the GESS assessment framework (10%).** For this, please refer to the scope of work in section 3.1 to ensure that your proposal falls within the expected parameters. Proposals will be assessed on how well they fit the listed requirements in the scope of work; therefore, we recommend ensuring that each bullet is addressed in your proposal.
- 2. An estimate of how many assessments your organization would be able to conduct within a year (10%).** In addition to the estimate, we are looking for a description of your capabilities that are sufficient to demonstrate that you would be able to complete the assessments (e.g., show that staffing levels are sufficient to meet your proposal).
- 3. Costs associated with conducting the assessments (40%).** A4L will not necessarily assign the most points to the lowest bidder; rather, we will consider how well the proposer balances

costs and rigor, helping ensure that smaller edtech providers that have typically not been able to afford a cybersecurity assessment will be able to participate.

4. **Background on your qualifications (30%).** We expect the firm to have experience performing cybersecurity assessments covering the frameworks that make up GESS (e.g., CIS, NIST). We also expect that the firm will have experience conducting rigorous assessments for businesses of varying sizes, but especially smaller businesses, being able to provide audits that are both rigorous and cost-effective. Please describe your organization's experiences in performing similar audits to the one in your proposal, especially highlighting how you balance cost and rigor. For this, evidence may include samples of past work, proof of technical skills (e.g., certifications), descriptions of successful engagements with similar organizations, or references.
5. **Description of how you maintain objectivity in assessments (10%).** The firm must maintain independence and objectivity, keep sensitive information confidential, and avoid conflicts of interest. Please describe how your organization has achieved this in other engagements and any controls or other procedures you follow.
6. **(Optional) Description of how your organization will help grow recognition of GESS as the global standard in K–12 education cybersecurity (Bonus 10%).** In order to help grow recognition and adoption of GESS throughout the K–12 school and edtech provider communities, we will award optional bonus points to proposals that describe how their organization will leverage their current position to help grow recognition, adoption, and acceptance of GESS among K–12 schools and the educational technology provider community.

5.3.1. *Scoring*

Proposals will be evaluated out of 100 points weighed based on the following criteria (a sample of the scoring sheet can be found [here](#)). Providing additional support for GESS adoption is not a requirement, but firms that address this in their proposal will be able to receive up to 10 bonus points toward their final score.

Evaluation Criteria	Weight
Assessment Framework Proposal	10%
Annual Assessment Capacity	10%
Cost & Rigor Balance	40%
Organizational Qualifications	30%
Objectivity & Conflict Avoidance	10%
(Optional) Support for GESS Adoption	+10% Bonus

6. Additional Legal Terms and Disclaimers

- Proposals are not binding until a contract is executed.
- A4L reserves the right to reject any or all proposals.
- A4L reserves the right to negotiate scope and cost.
- Proposals and materials submitted will not be returned.

- All work must comply with applicable laws and data protection regulations.
- All costs incurred in the preparation or submission of a proposal shall be entirely the responsibility of the assessment provider and shall not be chargeable directly or indirectly to A4L.

Budget Proposal Template

Company info	
Company name	
Company address	
Primary contact	
Name	
Title	
Address	
Phone	
Email	

Costs for framework development (Scope of Work 1)

Note: we expect that your proposal will contain the main details of a proposed framework. This would include any costs anticipated after an award to finalize the framework. If you do not anticipate any additional costs, please leave blank.

Cost Type	Cost Explanation	Projected Hours	Hourly rate	TOTAL
Total costs for framework development				

Labor costs per assessment (Scope of Work 2)

Job title / name	Explanation (e.g., role in project)	Projected Hours	Hourly rate	TOTAL
A. Total labor costs per assessment				
B. Estimated assessments per year				
C. TOTAL labor costs for year of assessments (A x B)				

Indirect / other costs

Cost Type	Cost Explanation	Projected Hours	Hourly rate	TOTAL
Total indirect / other costs				

Summary

Total costs for framework development	
Total labor costs for year of assessments	
Total indirect / other costs	
TOTAL cost of proposal	

We attest that prices quoted herein are valid for at least 120 days upon receipt by A4L