

REQUEST FOR INFORMATION

The A4L Community is seeking information from auditing/certifying firms regarding future third-party certification for its Global Educational Security Standard (GESS)

1. Overview

In 2025, the Access 4 Learning Community (A4L) plans to offer a third-party certification for its Global Educational Security Standard (GESS). We are currently seeking information from firms experienced in information security assessments or specialized in auditing and certifying products for their compliance with cybersecurity frameworks or standards to better understand what solutions certifying firms already offer. We also want to know what information these firms would need from us to scope out a more detailed road map for this project.

Please note that this Request for Information (RFI) is for informational purposes only, and no contract will be awarded as a result. A firm or organization's response to the RFI—or lack thereof—will have no impact on the evaluation of responses to any subsequent Request for Proposals (RFP) or Invitation to Bid (ITB) released. Responses will be used solely for information and planning purposes.

1.1 Contact Information

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

David Sallay, Director of Privacy | dsallay@a4l.org | (508) 202-0855

Please submit your responses to or questions about this RFI via email to the RFI point of contact before the due date identified in Section 1.2.

1.2 RFI Timeline

Please review the below RFI timeline. Dates may be modified or amended by A4L, which will post an amendment to this RFI notifying prospective respondents of any change. We also note that we plan to hold an optional conference call/information session on Friday, March 7, to allow prospective respondents the opportunity to ask clarifying questions.

RFI Released: **Friday, February 14, 2025**

RFI Conference Call/Information Session: [**12pm ET Friday, March 7, 2025**](#)

Deadline for Questions: **Wednesday, March 26, 2025**

Responses Due: **Friday, March 28, 2025**

2. Background

Started in 1997 by software vendors and schools collaborating, the SIF Association – now the Access 4 Learning Community – is a unique, non-profit collaboration composed of more than 3,000 schools, districts, local authorities, states, US and International Ministries of Education, software vendors 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 vendors that have agreed to the terms of the NDPA for their educational technology products (edtech).

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 all existing security frameworks, including the NIST CSF and CIS Controls, 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 part of this initial release, A4L offered a [self-assessment tool](#), which edtech vendors could use to determine their current posture related to the controls in GESS. In order to provide more robust assurance, we indicated that in the near future we anticipate that third-party security auditing, certification, or compliance organizations may partner with A4L to offer follow up reviews of self assessments.

3. Requested Information

Specifically, A4L seeks the following information:

- Background information on RFI respondents
 - Introduce the organization by sharing its history, size, background, etc.
 - Provide a description of the organization's past experience auditing and certifying products for their compliance with cybersecurity frameworks, standards, or controls.
 - Provide a description of the organization's past work with standards organizations, if any.
- Specific information on the types of audit engagements your organization could offer
 - Walking through the controls described in the GESS, describe what it would realistically require to provide assurance that the software vendor is following the control.
 - Identify any controls where providing assurance would be excessively costly and whether there are more affordable alternatives.
 - Provide a realistic timeline for a start-to-finish audit engagement.
 - Describe how a GESS audit may align to other audits your organization may already provide and the potential to supplement existing audits.
 - Describe how you balance rigor and cost.

- Software vendors that provide edtech may provide other products outside of schools; therefore, we are most interested in certifications on a product-by-product basis. Please describe your experience with evaluating products (as opposed to full enterprises).
- Describe the type of documentation that could be provided to the software vendor, to A4L, or to any of their clients (i.e., schools) at the end of an engagement.
- Describe steps your organization follows to ensure the independence of the audit.
- Describe steps your firm follows to maintain the security of sensitive information received from the software vendor both in transit and at rest.
- If applicable, please share any feedback you have received from software vendors that you have reviewed. If any feedback was constructive, please share how you have addressed it.
- Specific suggestions on providing and publishing a certification
 - Describe whether the funding structure for the certification program will impact how schools will view the quality/independence of the audit (e.g., the software vendor contracts directly with the auditing firm vs. A4L contracts directly with the auditing firm).
 - Describe how long certifications typically should be considered valid before a new audit should be conducted.
 - Our interest is to only certify software vendors that meet all of the controls without qualifications. From your experience, is this a reasonable expectation, or are there situations where passing with qualifications is appropriate? If so, what is a reasonable minimal standard? How do you communicate any qualifications to customers so that they are understood?
 - Certification obviously does not guarantee that a software vendor will never be the victim of a data breach, have a negative story published about them in the press, or have some other data incident that could suggest to the general public that the certification is not adequately reliable. What types of incidents should trigger follow-up investigation/review? When would it be appropriate to remove a software vendor's certification?