

How many of these assessments to expect in a year? Are they mandatory for your members?

There are no mandatory requirements to be a member of A4L. This would be for those vendors that were interested in pursuing a certification. Because of this, the expected number of GESS assessments is difficult to gauge. There are a number of factors that may influence this. First, is the fact that the GESS control set is a new set of controls that is being introduced to the EdTech marketplace. Second is the fact that there is a need to standardize the expected set of controls across the marketplace to ensure that all providers are in fact implementing the proper controls and that they can be held accountable. Third is the desire of districts to hold vendors accountable. We anticipate the pressure of our close to 7,000 participating school districts to begin requiring these controls, and proof thereof, over the next couple years to impact the adoption rate. Thus the eventual uptake could be very large, yet the initial update could be very slow allowing time to ensure the assessment process is sound.

Is there a set budget for the development of the framework?

We are hopeful that firms will be able to leverage and adapt their existing work to create an assessment framework specifically for GESS, but recognize that there will be the need to work out the details with A4L staff, which will take billable hours. The A4L Association Board will be approving any contract that is awarded as well as the associated expenses.

Will A4L have a point of contact to assist with the development of the framework?

Yes. We anticipate the awardee will work with A4L and the GESS project team to work out the details of the assessment framework. The point of contact for this will be David Sallay, Director of Data Privacy.

In developing the framework described in 3.1, you state that the framework should contain multiple tiers. Would this mean that at some levels we would only do some of the controls? Should each level contain all of them? Should we identify some controls as foundational for all systems?

As part of our RFI responses, most firms recommended multiple assessment tiers based on different factors, though typically always taking into account the amount of sensitive information they maintained and the sensitivity of that information. Edtech providers tend to vary widely on both counts. For instance, some may only maintain a basic student identifier (e.g., email address) and their math scores, whereas others maintain all of the student's academic information, behavioral, disciplinary and health records. Some systems contain sensitive information that is not personally identifiable (e.g., see the [Raptor data breach](#), where school safety plans and procedures were compromised). Another good example to look at would be the recent [PowerSchool breach](#).

Both Raptor and PowerSchool had received SOC2 certification despite missing some obvious security steps. Because of this, many in K-12 education are skeptical of how much they can trust a company's SOC2. For GESS, we would not say that each tier must contain every control, but we want to see a strong case for the different tiers to adequately cover the risk.

In 3.1, it says that assessments should be done on a product-by-product basis, not an enterprise, but that we should streamline so we wouldn't have to repeat the same process with a new product. Is this a contradiction?

To clarify, edtech providers will receive a badge for GESS certification on a product-by-product basis. If a provider were having multiple products certified, we recognize that some controls could be checked once at the enterprise level. If there are any other opportunities to streamline, we would love if you could identify it in your proposal.

In 3.1, you state that the framework should include a remediation window. This will vary depending on how far short the edtech provider is (being short 5 controls vs 100). Should it be the same across the board?

No, it is not necessary to be the same across the board. We want to ensure that vendors that are close to certification be given a chance to remediate without having to start over from scratch, but recognize that there will be cases where this won't be realistic. Please address how you would recommend making this determination in a way that balances cost, rigor, and fairness.

In 3.1, you mention that the framework may be used by additional cybersecurity firms. Is that going to be determined during this RFP process?

Although we anticipate opening up this opportunity to more than one auditing firm, we anticipate starting with one organization to build the assessment framework and then eventually, depending on demand, opening up to other auditing firms. At that time a quality assurance program would need to be put in place by A4L to ensure all auditing offerings are of the highest quality.

In 4. where you discuss the budget, you mention revenue sharing with A4L. Should we incorporate this into our budget proposal?

For your proposal, it would be most helpful if you would identify what the costs will be on your end. This will be the most helpful for us to evaluate. Details of the revenue sharing will be worked out after with the awardee.

In 5.2.6, we are asked to identify pricing. Should we note maintenance costs for once the program is successful and needs to scale?

Yes, please identify costs you believe will be necessary as the program goes on, particularly for solutions that may be needed as more and more vendors come on (e.g., GRC tools). In this case, we would recommend providing a suite of options with your proposals to help us plan out for the future success of the program (e.g., what would be the bare minimum necessary, what would be at industry standard levels, what would exceed industry standard levels).