Emerging Compliance Risks for Community Developed Software

Background

Columbia University has recently formalized accessibility requirements for university websites (***emphasis added***):

> ***New or substantially revised content***: All content that is created or undergoes substantial revision after the effective date of this Policy is required to conform to the Accessibility Standard. In addition, ***Site Owners who manage University Websites that are maintained, upgraded, or updated by vendors are required to ensure that the vendor-provided design, code, and content meet the Accessibility Standard when the contract is entered into or renewed***.

We have also begun to receive requests from partner universities for accessibility documentation around subscription/collaborative databases (***emphasis added***):

> As a state institution, [redacted] are now being required to review all of our vendors to see if they will fall under the umbrella of companies which will need to receive the Texas Risk and Authorization Management Program (TX-RAMP) certification. Information on TX-RAMP may be found here: https://dir.texas.gov/sites/default/files/2022-01/TX-RAMP%20Overview%20Webinar%20For%20Vendors.Update.pdf
>
> We have some questions that will help our ITSS department determine if your platform will need to be TX-RAMP certified and at what level.
>
> 1. Are your services hosted locally, or do you use another platform (e.g., Amazon Web Services)? If hosted locally, where is your private cloud physically located?
> 2. ***Have you contracted with any 3rd parties to perform penetration testing on your services?***
> 3. What data is stored from our users in your systems?
> 4. What types of security measures are in place to protect the data in question? (encryption at rest and in flight, for example)
> 5. ***Does your platform have a VPAT or other accessibility statement you can provide to us?***

Please note that we will not be permitted to renew any subscriptions or purchase further products until a determination has been reached and certification achieved if applicable.

Risks

At Columbia we are tracking documented accessibility compliance for key OSS platforms (OJS (PKP), WordPress, IIIF clients, and Blacklight) in the context of projects that constitute a "substantial revision" of our web properties.

There is a risk that, as such policies become more common (particularly at publicly-funded institutions, or where legal action has resulted in blanket policies), platforms without a process to document accessibility and security reviews will become subject to "regulatory exclusion".

Questions

- Are other partners facing similar compliance efforts around accessibility?
- How are community-developed tools being reckoned in the scope of those policies?
- Do the policies in question emerge from external entities with oversight responsibility, or internally?
- How should accessibility review & reporting be handled for platforms where local customizations and locally-managed content bear as much or more on compliance as the platform UI?
- How is the Samvera community approaching this problem for its products?
- How might such reviews be organized for the less formally organized project underpinning Samvera efforts?
- Is there an opportunity for the Samvera community to model behavior in this area even where compliance is voluntary/not (yet) compulsory?

Glossary

VPAT: Voluntary Product Accessibility Template (VPAT®)
ACR: Accessibility Conformance Report, a document describing the WCAG conformance level and the evaluation mechanisms used to establish it. See also How to Create an Accessibility Conformance Report Using A Voluntary Product Accessibility Template (VPAT®)