How does Cyber Crucible support GLBA and financial-institution vendor requirements?

Short answer: As a software service provider to a financial institution, Cyber Crucible supports the institution's obligations under the GLBA Safeguards expectations and the interagency information-security guidelines — primarily by never collecting the non-public personal information (NPI) those rules are written to protect. Cyber Crucible is a software vendor, not a chartered financial institution, so it is not itself examined; its controls are built to be examinable as part of the institution's third-party risk program.

Where the architecture does the work

- **No NPI collected.** The product runs on endpoints that may handle NPI without extracting it. There is no consumer financial information for Cyber Crucible to use, share, or re-disclose, which directly supports the GLBA Privacy Rule / Regulation P position.
- **Documented security program.** Access control, encryption, breach response, and change control are documented and evidenceable — the safeguards a bank's program looks for in a service provider.
- **Due-diligence evidence on hand.** A prepared vendor package is structured to serve as the due-diligence and ongoing-monitoring evidence a bank needs under current interagency third-party risk guidance.

The honest boundary

Cyber Crucible supports a customer's compliance obligations; it does not, by itself, make an organization compliant, and this is not legal advice. Specific, evidence-grade detail is provided to a bank's reviewers under NDA. See also *Does Cyber Crucible meet FFIEC and third-party risk management expectations?*

Revision #2
Created 2026-07-23 15:18:07 UTC by Dennis Underwood
Updated 2026-07-23 18:19:38 UTC by Dennis Underwood