Gramm-Leach-Bliley Act

GLBA

The Safeguards Rule

Key Elements/Safeguards

- Designation of a qualified individual for security program oversight.
- Conduct a written risk assessment.
- Implement and periodically review access controls.
- Know what you have and where you have it.
- Encrypt customer information, whether static or transit.
- Development of secure in-house or third-party apps to reduce risk to data.
- Implement two-factor authentication.
- Dispose of customer information securely.

Key Elements/Safeguards Cont.

- Adoption of change management polices.
- Implementation of procedures and controls to monitor and log authorized user activity.
- Regularly monitor and test the effectiveness of your safeguards.
- Train employees regularly.
- Monitor service providers.
- Create a written Incident Response Plan.
- Mandatory reporting to Board of Directors (Trustees).

Risk Assessment

October 2022, Tandem Cybersecurity, performed a Risk Assessment for the college, focusing on Gramm-Leach-Bliley Act (GLBA) requirements.

Risk Assessment Report was provided, March 31, 2023.

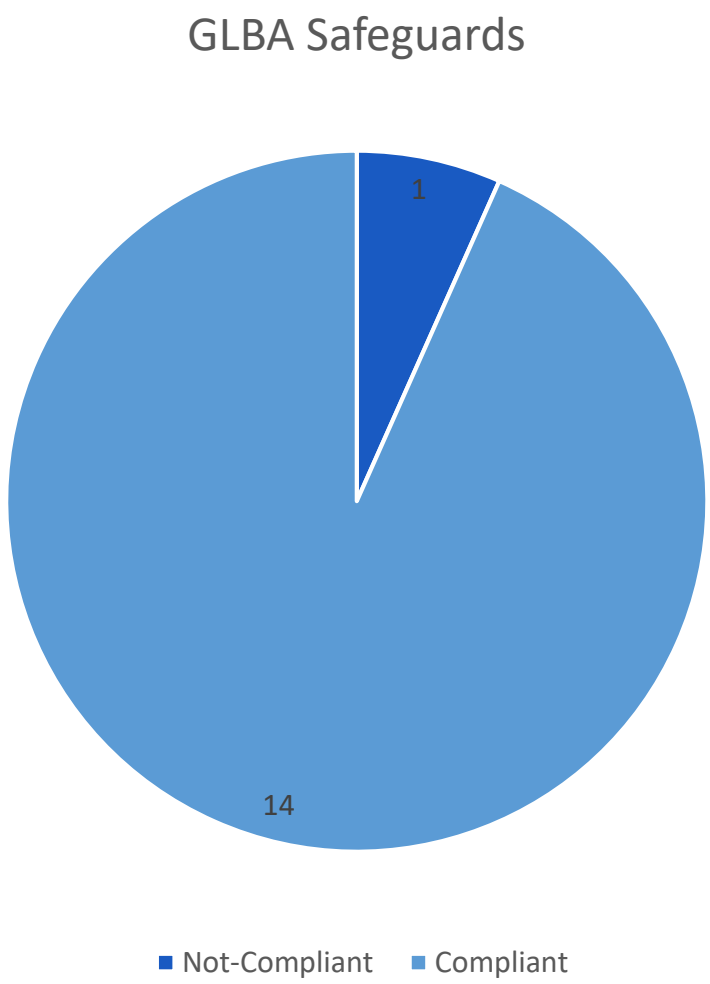
Assessment Methodology

The assessment involved a comprehensive review of the following information about the organization – assets that process sensitive data, technical and administrative controls, policies, and procedures. To ensure compliance with the Gramm-Leach-Bliley Act (GLBA), Tandem Cybersecurity, reviewed the Center for Internet Security (CIS) controls and the Federal Trade Commission's (FTC) GLBA safeguards.

Risk Assessment Results

Out of the 15 Gramm-Leach-Bliley Act (GLBA) elements/safeguards, the college met 14. The 1 not completely met, was a consistent way to monitor our service providers. In other words, we need to have our service provider's contracts spell out our security expectations and ask the vendors to contractually state that they do safeguard our data.

Note: Before the risk assessment, we had already started asking our vendors if they store any PII data, where the data is stored and what controls they have in place to secure our data. Vendors storing data, are providing electronic statements of where the data is and how they are following GLBA regulations (safeguards). We are currently working on a statement, that we will be asking vendors to include in contracts.



Questions?