GLBA and Cyber Risk Assessment

June 10, 2025

Executive Summary

As digital information evolves, cybersecurity threats pose significant and immediate risks to the college. As stewards of sensitive information, the college has committed to a comprehensive cyber-risk assessment and a thorough audit of its safeguards as mandated by the Gramm-Leach-Bliley Act.

This initiative is a regulatory requirement and a strategic imperative to protect the organization and students from malicious cyber activities and data breaches. In collaboration with the college staff, Tandem Cyber has conducted an assessment that evaluated the compliance of Barton Community College with the Gramm–Leach–Bliley Act and then conducted a risk assessment. This report outlines the findings from both efforts.

Assessment Methodology

The assessment methodology 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 reviewed Center for Internet Security (CIS) controls and the Federal Trade Commission's (FTC) GLBA Safeguards.

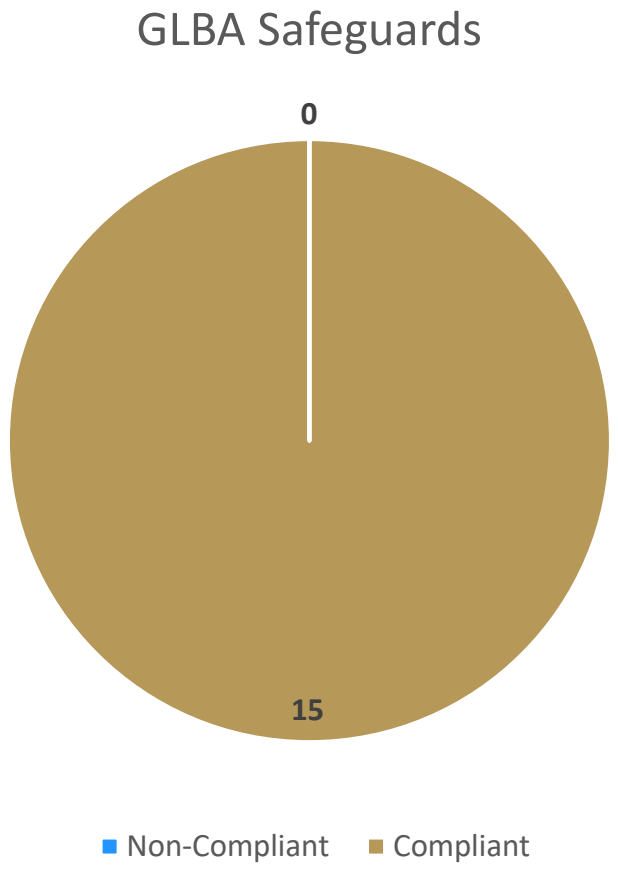
The results of the control review were used to conduct a risk assessment in accordance with GLBA requirements. Risk profiles are defined as Acceptable, Unacceptable, and Catastrophic. The risk profiles are measured based on the aggregate risk levels of controls Risk = Max (Mission Impact, Objectives Impact, Obligations Impact) x Likelihood, per control.

This methodology allowed for a thorough evaluation of the organization's information security posture and helped to identify any gaps or vulnerabilities in its systems and practices. The assessment report provides recommendations for addressing identified risks and ensuring ongoing compliance with GLBA regulations.

GLBA Safeguards

Gramm–Leach–Bliley Act safeguards, 15 of the 15 safeguards were compliant.

As a result, Barton's environment is compliant with the Gramm–Leach–Bliley Act Safeguards and Barton is at a low risk level.



GLBA
15 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.

GLBA
15 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).

Cyber Risk Assessment
CIS Controls

The Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.

There are 18 CIS Controls, which are broken up into three Control Groups and within the 18 controls are 153 Safeguards. The 153 Safeguards are a set of specific, actionable measures designed to mitigate the most common and impactful cyber threats. Each Safeguard has a targeted "Asset Type" with a specific "Security Function".

Information Services have worked through the Implementation of Control Groups 1 (56 safeguards) and 2 (74 safeguards) and have met those 130 safeguards. With the latest risk assessment, we started the review process for Implementation Control group 3 (23 safeguards.) We currently meet 133 out of 135 that are applicable to the college. 18 safeguards are not applicable at this current time.

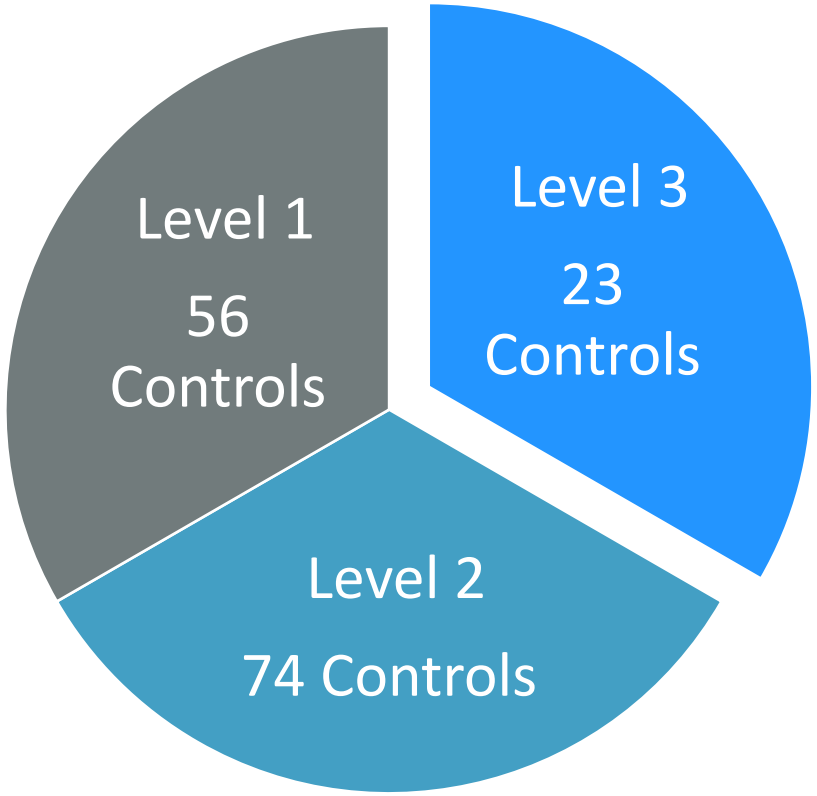
Center for Internet Security (CIS) Controls v8

There are 153 CIS v8 safeguards total.

Barton has 133 of the 135 safeguards either fully or partially implemented.

Currently 18 safeguards are not applicable for Barton.

[CIS Critical Security Controls Version 8]



Cyber Risk Assessment
Findings and Recommendations

- Allowlist for Authorized Scripts – ensure that only authorized scripts are allowed to execute.
- Enforce Data Retention – Automating retention standards to help ensure that sensitive data is not kept longer than necessary.

Conclusion

The recommendations covered will ensure that Barton complies with critical cybersecurity controls meant to protect the scoped sensitive data.

Questions?