# The Gramm-Leach-Bliley Act: What Higher Education Institutions Need to Do Now

By Daniel M. Campbell, Partner

Given the increasing and rapidly changing risk, cybersecurity should be a key focus for all higher education institutions.

Institutions collect and store a wide variety of data across many departments, ranging from health and financial information to intellectual property. Students and their families, employees, and the general public have high expectations for how your institution safeguards sensitive information. A breach can have significant and long-lasting repercussions for your institution's operations, finances, reputation, and public trust.

While this affects all institutions, those that participate in Title IV programs face additional information security requirements. These institutions are considered financial institutions under the Gramm-Leach-Bliley Act (GLBA), which includes privacy and information security provisions to protect individuals' personal information.

While GLBA requirements are not new, they are now part of the required audit procedures in the Compliance Supplement. Read on to learn more about the changes, the steps you need to take, and the potential cost of noncompliance. And if you're not a Title IV institution, the information below can help you tighten up your cybersecurity defenses.

**How GLBA Requirements Apply to Higher Education**

GLBA contains six key provisions for higher education institutions to address:

1. Developing, implementing, and maintaining a written information security (InfoSec) program
2. Designating the employee(s) responsible for coordinating the InfoSec program
3. Identifying and assessing the risk to customer information
4. Designing, implementing, and regularly testing and monitoring information safeguards
5. Selecting appropriate service providers that are capable of maintaining appropriate safeguards
6. Periodically evaluating and updating the InfoSec program

**What Changed — and How it Might Affect Your Institution**

The United States Department of Education Financial Student Aid (USDE FSA) Program Participation Agreement (PPA) and Student Aid Internet Gateway Agreement (SAIG) require Title IV institutions to have GLBA safeguards in place. The president of the institution already signs the PPA, which includes a statement that the institution will comply with GLBA.

However, every year the Office of Management and Budget (OMB) issues the Single Audit Compliance Supplement. This acts as a guidebook for single audits of all non-federal entities that expend $750,000 or more in federal funds in a single year. The 2019 Compliance Supplement issued July 1, 2019 for fiscal year-ends of June 30, 2019 and beyond includes required audit procedures related to GLBA.

**This means that institutions will be audited to verify that they have taken these steps:**

1. Designated an individual to coordinate the InfoSec program
2. Performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4(b), which are:
    a. Employee training and management
    b. Information systems, including network and software design, as well as information processing, storage, transmission, and disposal

c. Detecting, preventing, and responding to attacks, intrusions, or other systems failures

3. Documented a safeguard for each risk identified during step 2

**Understanding the Risks**

Any deficiencies identified during the audit procedures would be evaluated under the administrative capability criteria. Keep in mind, too, that any reportable findings would be publicly available. This includes the full context of the finding, since changes in the data collection form are also effective.

An administrative capability finding (i.e., unable to properly administer Title IV funds) would require a corrective action plan from the institution. Repeat findings with the Department of Education can lead to termination of participation in Title IV funding.

**Next Steps**

As noted above, even if the GLBA requirements don't apply to your institution, they can help reduce your cybersecurity risk.

It is anticipated that the remaining components of GLBA will be added to future compliance supplements. Now is a good time to evaluate whether:

- The written information security program is robust and complete,
- Service providers have been adequately vetted and that vetting has been documented, and
- The information security program is functioning as intended through periodic review.

After the risk assessment has been completed, any residual risks above a low rating would likely want board approval. It also may be prudent to seek insurance coverage for residual risks.

If you'd like assistance in this area, the team at CapinTech has been helping organizations comply with GLBA for 20 years. We can provide a sample policy and help you identify and implement appropriate safeguards. Please contact us at cybersecurity@capincrouse.com to learn more.

*This article was originally published in Christian Academia magazine.*

## About the Author

**Daniel M. Campbell, Partner**
Higher Education Services Director
dcampbell@capincrouse.com
o 505.50.CAPIN ext. 1452

Dan has more than 35 years of public accounting experience leading audit engagements of nonprofit organizations and for-profit industries. Dan leads the firm's higher education practice segment, which includes more than 80 client relationships, and commits a significant portion of his professional time to board training, strategic planning initiatives, and accreditation support. He served on the Board of Trustees of Davis College for 25 years. Prior to joining the firm in 2006, Dan managed audits of financial institutions, construction contractors, and manufacturers.

## About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.