CAPINCROUSE LLP

Higher Education Institutions Face Increased Scrutiny of Cybersecurity Measures

By Daniel M. Campbell, Partner

Information security audit procedures expected in 2018 USDE Single Audit Compliance Supplement.

Cybersecurity should be a top priority for all higher education institutions. Public expectations for information security safeguards are high, and data theft or compromise can have a serious impact on your institution's finances, operations, and public trust.

In addition, higher education institutions that participate in Title IV programs face additional information security requirements.

Additional Requirements for "Financial Institutions"

Higher education institutions that participate in Title IV programs are considered financial institutions under the Gramm-Leach-Bliley Act (GLBA),[1] which includes consumer financial privacy provisions. (Activities that are financial in nature include lending activities and the electronic transfer of funds to customers.)

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. **Institutions without GLBA safeguards may be found administratively incapable**, i.e., unable to properly administer Title IV funds.

Key components of the GLBA requirements include:

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

While GLBA requirements are not new, they continue to gain attention as more records and interactions become digital.

While GLBA requirements are not new, they continue to gain attention as more records and interactions become digital. Institutions of higher education (IHEs) are targeted because they are depositories of significant volumes of controlled unclassified information (CUI), primarily personally identifiable information (PII). For example, CUI information of parents and students includes:

- Name
- Date of birth
- Social Security number
- Address
- Email address
- Phone number
- Income tax information

Data security is a business risk, which means everyone is responsible. The president signs the PPA and SAIG. The chief information officer, chief information security officer, and staff implement and monitor information safeguards. The CFO and business office direct the electronic transfer of funds. Admissions and financial aid staff collect data. Registrars maintain data. Faculty and staff submit and have access to data. Parents and students submit data. Everyone should be concerned with data security.

New Information Security Audit Procedures on the Horizon?

Additional changes are likely. Each year, the Office of Management and Budget (OMB) issues the Single Audit Compliance Supplement, which 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 2018 Single Audit Compliance Supplement is expected to require new audit procedures of information security safeguards maintained by institutions of higher education that participate in Title IV federal student aid programs.

Data security is a business risk, which means everyone is responsible.

The Compliance Supplement is normally issued during the summer months and is effective for fiscal years beginning after June 30 of the previous year. The 2017 Compliance Supplement is available here, and the U.S. Department of Education (USDE) section of the compliance supplement is in Part 4.

In accordance with the July 29, 2015 Dear Colleague Letter GEN 15-18 and July 1, 2016 Dear Colleague Letter GEN 16-12,[2] the 2018 supplement is expected to address provisions of the GLBA that pertain to protecting student PII.

According to the Federal Student Aid office of the USDE,[3] starting in 2018, GLBA information security safeguards will be audited to ensure administrative capability. Draft audit language may include:

> **Audit Objectives** – Determine whether the IHE designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.
>
> **Suggested Audit Procedures**
>
> a. Verify that the IHE has designated an individual to coordinate the information security program.
> b. Obtain the IHE risk assessment and verify that it addresses the three required areas noted in 16 CFR 314.4 (b). The three areas are:
>   i. Employee training and management
>   ii. Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
>   iii. Detecting, preventing and responding to attacks, intrusions, or other systems failures.
> c. Obtain the documentation created by the IHE that aligns each safeguard with each risk identified from step b above, verifying that the IHE has identified a safeguard for each risk.

Next Steps

Where should you go from here?

- Locate your institution’s information security program. If you don’t have one, develop one. Verify that your institution’s information security program identifies a responsible individual and contains their contact information. Be certain to keep information updated in the program.
- Verify that your institution has an information risk assessment and testing schedule in place. If you don’t have one, develop one.
- Verify that your institution has documented the risk assessment, testing, and results. If the risk assessment has not been tested, start following the schedule and documenting.
- Add your information security program, schedule, and contact information to your consumer information and compliance website so you can easily maintain it.
- Communicate your response plan to your entire board and executive team so everyone is prepared to respond to a breach immediately and appropriately.
- Consider insurance coverage that corresponds to the identified risks.
- Consider developing a professional relationship with legal counsel who is familiar with breach reporting requirements in each state in which you do business.

Planning for and implementing these standards will help your institution maintain compliance and protect your data. Please contact us with questions or to discuss how we can assist your institution with compliance and reducing your cybersecurity risk.

About the Author

Daniel M. Campbell, Partner
Higher Education Services Director
dcampbell@capincrouse.com
o 803.458.2169
c 404.931.7287

Dan has more than 30 years of public accounting experience leading audit engagements of nonprofit organizations and for-profit industries. He has served on the Board of Trustees of Davis College since 1993. 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.

[1] "Cyber Security For Title IV Schools: How Being A "Financial Institution" Changes The Paradigm," Office of the Inspector General, U.S. Department of Education Technology Crimes Division, pg. 6; available at https://www.ren-isac.net/events/attachments/TB_Apr21_2017.pdf
[2] Ibid.
[3] "Postsecondary Institution Data-Security Overview & Requirements," Presentation, 2017 FSA Training Conference for Financial Aid Professionals