GLBA: Where We Are Now

By Allison Davis Ward, Partner

The Gramm-Leach-Bliley Act (GLBA) is not new. When signing the Program Participation Agreement to receive federal funds, higher education institutions acknowledge their compliance with GLBA. And the Federal Student Aid (FSA) Office released notices in July 2015, July 2016, and February 2020 reminding these institutions of their requirements to protect the personally identifiable information (PII) of their students.

However, many institutions are still struggling to become fully compliant. While this is likely related to the lack of formal assessment in the past, audit teams are now evaluating various components of GLBA as part of Uniform Guidance audits. So it's time to get compliant.

And even if you're not a Title IV institution required to comply with GLBA, the information below can help you tighten up your cybersecurity defenses and better protect your sensitive data.

Consider What GLBA Noncompliance Could Mean for Your Institution

Noncompliance could have significant ramifications. Your auditors are now required to include a finding in your audit report. That finding is then referred to the Federal Trade Commission (FTC) and the FSA's Postsecondary Institution Cybersecurity Team, either of which may request additional information to determine the risk to the PII at your institution.

Consider the potential financial and reputational impact of this finding in your audit report:

- Fines, penalties, and ultimately a loss of federal funding could be imposed.
- If you don't have insurance to offset the fines, disclosure may be required in the financial statements, depending on the nature of the fines and the timing, magnitude, and likelihood of realization.
- Your ability to secure sensitive information could be called into question. That could affect enrollment or donations if your constituents feel you can't meet baseline requirements to secure their information.
- The finding is publicly available through the Federal Audit Clearinghouse website.

The potential impact of a loss of federal funding or reputation damage highlights the importance of striving for full compliance at your institution quickly.

The potential impact of a loss of federal funding or reputation damage highlights the importance of striving for full compliance quickly. The longevity and reputation of your institution are at stake.

The standards for higher education institutions are in 16 CFR 314.4. Let's walk through why GLBA can be a challenge, define what is required for immediate and long-term compliance, and discuss resources that can help you get there.

The Difficulty with the Guidance

GLBA, like many other sources of guidance, is relatively vague, and that can be a double-edged sword. The vagueness recognizes that not every entity operates the same and allows institutions of varying sizes and complexities to implement it in the way that is most effective for them.

However, this vagueness can make it difficult for institutions to know where to start. And what is deemed acceptable for meeting the guidance today can change. In addition to serving higher education institutions, for over 20 years CapinTech has worked with financial institutions, which operate in a heavily regulated industry and must meet GLBA requirements. Over the years, various components of GLBA have come to mean very specific things as regulatory agencies have inspected financial institutions. We expect that compliance within higher education will follow this trend and become more defined as we move further into the assessment phases of compliance.

The Immediate GLBA Requirements

As part of the current OMB Compliance Supplement that governs the audits for clients with years ended June 30, 2020 through May 31, 2021, there is a subset of GLBA

that must be evaluated. Auditors have to determine whether the institution has:

- Appointed an individual responsible for overseeing the implementation of information security program efforts, and
- Conducted a formal assessment of risks to student PII and the safeguards that mitigate those risks.

Let's take a look at these components in detail.

Responsibility for the Program

Appointing responsibility for your information security program efforts is often fairly easy to achieve. But there are a few things to consider when making this decision.

- **Consider the individual's role and authority within the institution**. Most institutions assign this role to a C-level employee as they often carry great weight throughout the institution. While this is not required, you still want someone who has the authority and influence needed to effectively implement your information security program.
- **While the guidance doesn't require a formal appointment, we recommend formalizing this position through Board or C-level approval.** This is expected in other regulated industries. It also provides support for the goals and objectives the individual in this position will hold.
- **The appointed individual does not have to perform all the duties**. While this position is ultimately responsible for overseeing the various components of compliance, the actual implementation of each part can involve delegation of duties to individual staff members or committees. Given the number of aspects of the business that information technology touches, gathering data from multiple departments improves the effectiveness of the program.
- **The position does not have to be independent**. Many institutions are appointing their IT manager or director, but separating information security (InfoSec) and IT roles can be extremely beneficial because they have different purposes. For financial institutions, this requirement is interpreted as an independent information security officer position, and the same may happen in the higher education sphere as a result of increased scrutiny.

  However, at this time, we'd advise you to ensure that the most effective person performs this role to get your program off the ground. If you're appointing someone with no general knowledge of information security risks just for the sake of achieving independence, you're likely doing your institution a disservice.

Assessing and Mitigating Risk

The second major component your institution needs to consider is the detailed and documented assessment of risks to student PII. This can be a large project, depending on the size and complexity of your institution, but it's achievable in steps.

1. **Identify sources of student PII.** This is arguably the most critical part of this assessment. You can't manage what you can't measure, so it's necessary to identify all sources of PII. Some are clear, such as the student information system, the payroll application for student workers, reporting agencies such as the U.S. Department of Education's Common Origination and Disbursement (COD) site and the National Student Loan Data System (NSLDS), online enrollment systems, and student health centers or pharmacies. We recommend multiple people review the systems they use and the way data is transmitted to document all sources of PII.

   However, some sources are less evident. Consider applications and technology that don't directly hold student information but could grant access to other areas that house it, such as:

   - Remote access technology
   - Backup applications and technology
   - Network authentication and file shares
   - Email, encryption, and file-sharing systems
   - Password management systems
2. **Detail the risks to the information identified in Step 1.** What risks are posed to these applications and how can they affect the student PII? Common risks include unauthorized access due to physical theft or electronic compromise, data corruption or loss, and vendor breach and unavailability.
3. **Map those risks to migrating controls.** Fully document your risk mitigation efforts, such as policies, procedures, personnel training, application controls, user access management, segregation of duties, monitored activity, backup processes, and any other controls in place.
4. **Expand on general technology risks and controls.** Once you've identified these major sources of PII and threats, consider including enterprise-wide threats in your assessment (e.g., malware such as keyloggers and ransomware, outdated and obsolete applications, configuration vulnerabilities, social engineering, targeted hacking, and natural disasters). These threats could affect your institution as a whole, and ultimately your student PII due to the inherent nature and interconnectedness of a network.

Once completed, revisit this assessment annually. Threats and risks are constantly evolving so this should

not be a stagnant document. Instead, it should change and evolve with the threats.

Long-Term GLBA Compliance

It's important not to overlook the remaining aspects of GLBA that are not covered by the current OMB Compliance Supplement. While not audited this year, you still attested to full compliance, and future periods may require auditors to consider these other components.

You should familiarize yourself with the remaining areas and continue to work toward full compliance. These steps can help:

1. **Formalize and document your information security program efforts**. This documented program should expand upon your risk assessment and essentially define all of your efforts for securing student PII, from creation to destruction. Be sure to incorporate incident response guidelines, as planning for incidents can help minimize the impact to PII.
2. **Implement employee training and awareness efforts**. Your employees are your largest, and often riskiest, asset. It's important to ensure your staff understands their role as part of your control framework for protecting your students.
3. **Consider vendors that access, store, or transmit your student PII**. Vendors are an extension of your institution. It's critical to consider the risks they pose when developing your program. Establish processes to ensure these vendors maintain the same or better standards you do for GLBA purposes. This is often achieved through contractual requirements, formalized processes for initial due diligence of new vendors, and ongoing monitoring processes. Now is a great time to reevaluate vendors to assess any significant changes that may have been made as a result of the pandemic.
4. **Establish procedures to monitor the effectiveness of your program**. Again, so much can change from year to year. Therefore, having a way to test the effectiveness of your controls on an ongoing basis is critical. In the banking industry, this has specifically come to mean an independent, annual, third-party audit. However, the guidance does not specifically state that independence is required. So if an outsourced audit isn't feasible this year due to budgetary constraints, document everything you're doing internally to monitor components of your program, whether that's formalized internal audits, review of activity logs, or ongoing user access reviews. Watch our recorded webcast on prioritizing security during budgetary constraints for more suggestions for implementing and monitoring various controls.

What We Can Do?

If you are currently noncompliant with GLBA, do not stress! CapinTech has numerous resources available if you want to tackle compliance yourself. We have template programs and guidance that we are happy to share upon request. The resources linked throughout this article can provide additional guidance on various areas. And for some institutions of higher education, a half-hour video or phone call can help pinpoint specifics on how to get started and streamline resource deployment.

If you need more assistance or want a dedicated partner to walk through this process with you, CapinTech offers a variety of services to help you meet your GLBA compliance needs. This includes:

- **Risk assessment services** to identify and document reasonably foreseeable risks to your covered information.
- **Information Security Program development services** to help formalize and document your institution's security efforts to protect constituent information.
- **Vendor management services** to help define procedures for ensuring vendors that access, store, or transmit covered information on your behalf maintain similar standards and controls. We also can assist with the implementation of your vendor management program by performing document collection and review of policies, procedures, and security reports from your vendors.
- **Training services** to ensure your employees understand current threats to covered information and their responsibilities for securing it. We can provide seminars, conference sessions, and webinars for applicable parties, including executives, directors, managers, IT personnel, staff members, and other constituents.
- **Cybersecurity assessment services** to help you test the ongoing effectiveness of your defined Information Security Program. These services range from general controls reviews to more technical assessments containing vulnerability scans and penetration tests. Regardless of the type of assessment chosen, we can help you identify weaknesses in controls and configurations that could leave your sensitive data vulnerable to exposure.

Contact us at cybersecurity@capincrouse.com to learn more about how we can assist you with GLBA compliance.

About the Author

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

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.