GLBA Requirements for Higher Education Institutions and an Introduction to Risk Assessments

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Create Opportunities

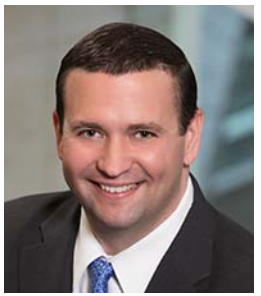
Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Learning Objectives

- Outline GLBA's specific requirements as they relate to the higher education industry
- Identify what is required in the Compliance Supplement as it relates to Student Financial Aid and what could potentially be included in the future
- Describe the GLBA risk assessment process and key steps required in the risk assessment

Speaker Introductions



Brian Pye

- Principal
- More than 20 years of experience
- Provides internal audit and information security services for higher education, governmental entities, and financial institutions
- Experience in risk assessments, IT general controls review, and internal auditing outsourcing

Speaker Introductions

Kadian Douglas

- Principal
- More than 12 years of experience in the industry
- Provides information security services for higher education, governmental entities, and financial institutions
- Experience in risk assessments, IT general controls review, and internal auditing outsourcing for financial and operational audits

Question #1

What year end describes your institution?

a. Prior to June 30
b. June 30 and later

What is GLBA?

- The Gramm Leach Bliley Act (GLBA) was first developed for and is applicable to “financial institutions” and requires that customer information is secure and confidential
- Colleges and Universities are considered financial institutions under GLBA.

GLBA Requirements

- Pretexting Rule
  - Addresses access to information under falls pretense
  - Addressed under the Red Flags rule
- Privacy Rule
  - Protection of and security of nonpublic information
  - If the institution is following Family Educational Rights and Privacy Act (FERPA) regulations this would address the privacy rule
- Safeguarding Rule
  - Addresses information security policies, risk assessments and controls in place mitigate identified risks.

Higher Education GLBA Requirement References

- The following includes documentation regarding the requirement for higher education institutions to be compliant with GLBA safeguards
  - Program Participation Agreement (PPA)
  - Federal Student Aid (FSA)
  - Student Aid Internet Gateway (SAIG)

2019 Fiscal Year Compliance Requirement

- The Institution has designated an individual to coordinate the information security program

- Institution has performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4

- Institution has documented a safeguard for each risk identified

Potential Future Addition

- Monitoring of third party service providers

- Potentially performing GLBA compliance in other processes/departments within the institution

Detail of the Risk Assessment Requirement

- Institution has performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4
  - Employee training and management
  - Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
  - Detecting, preventing and responding to attacks, intrusions, or other systems failures

What is a Risk Assessment?

- A systematic process for utilizing professional judgments to evaluate probable adverse conditions and/or events and their potential effects on your organization.

- A process for risk identification and prioritization of the higher education institution's key business risks (i.e. operational, financial, strategic).

Question #2

Do you use a formal risk assessment process at your institution?

a. Yes
b. No

Why is a Risk Assessment important?

- Why is a Risk Assessment Important?
  - Proactive approach to removing potential barriers
  - Helps the institutions focus resources
  - Helps identify unknown risks

Question #3

- Identify a risk that impacts your institution

Major Types of Risk and Risk Areas (Examples)

Department for an Information Security Risk Assessment

The risks associated with collecting , storing and processing students data

- Admissions
- Registrar
- Student Financial Aid
- Student Services
- Academic Affairs
- Facilities
- Bursar
- Human Resources
- Health Services (clinic)
- Athletics
- Marketing and communications
- Operations and Auxiliary Services (bookstore, food services)

Major Types of IT Risk and IT Risk Areas (Examples)

IT computing environment

Risks associated with the organization's IT systems

- Hardware
- Software
- System interfaces
- Databases
- System and data criticality (system's importance to the organization)
- System and data sensitivity
- Data backup and recovery process

Logical access

- Password Administration
- Direct access to data
- Physical access to data centers/facilities/equipment
- Lack of segregation of duties

Network security and availability

- System security policies
- System security architecture

Operational environment of IT systems

- Functional requirements of IT system
- Users of the IT system
- Management of data changes

Execute Risk Assessment Approach

- **Planning & Data Gathering**:

  Validate objectives, scope, and approach; understanding of expectations, develop a project plan, etc.

- **Interviews / Surveys**:

  Identifying various participants, including key process owners and conduct interviews and/or surveys. Key risks are gathered and documented during this stage.

- **Ranking of Risks**:

  Using the risk model we rank each identified risk as high, moderate, or low based on the defined impact and vulnerability criteria.

- **Validation of Risks**:

  Discuss and validate all risks identified, including risk rankings and recommendations with the institution.

- **Reporting Results**:

  Develop a report that is inclusive of the risk assessment methodology; the scope, objectives, and approach taken; and the specific risks identified including recommendations and risk ranking.

Identify and Analyze Risks

- Criteria for selecting Auditable Units:
  - Collects, store, process and share student sensitive and confidential information
- Risk forms:
  - Inherent
  - Residual

Identify and Analyze Risks, cont'd

- Define the Objectives Universe
  - Start with protecting and safeguarding student sensitive and confidential information
  - Determine alignment with organization's overall mission/vision
  - Categories of objectives
    - ◊ Reliability and integrity of information
    - ◊ Effectiveness and efficiency of operations
    - ◊ Safeguarding of assets
    - ◊ Compliance with laws, regulations and contracts

Identify and Analyze Risks, cont'd

- Define the Risk Universe
  - If you don't identify it, you can't measure, prioritize or manage it
  - Dependencies for success:
    - ◊ Thorough understanding of auditable units
    - ◊ Process to generalist list of possible risks
      - Risk framework
      - Questionnaires, Interviews
      - Prior Audit Results
      - Industry data

Identify and Analyze Risks, cont'd

- Define the Risk Universe, cont'd
  - Use of a Risk Framework
    - ◊ Exposure Analysis –from the perspective of the primary assets of the organization (physical, financial, human and intangible)
    - ◊ Environment Analysis –from the perspective of changes to external environments and their effects on management processes and controls
    - ◊ Threat Scenarios/Brainstorming – How internal control could be defeated by fraud or natural disaster

Identify and Analyze Risks, cont'd

- Reassess the Audit Universe
  - Additional information is often needed
  - Validation occurs
    - ◊ Review of Chart of accounts, Org chart, Telephone directory, Strategic Plan, Inventories, Audit Requests, External Benchmarking

Measure Risks

- More Art than Science
- Focus on overall objective; identification of high impact audits and program design
- Qualitative measurement most effective (High, Medium, Low)

Measure Risks – Score Risk Factors

- Choose Scoring Scale
- Establish criteria for rating
- Evaluate for strength and/or presence
- Calculate overall score
- Identify Total Risk

Impact on Controls

- **Facilitate Process and Internal Controls Discussions**
  - Discussions with key managers and stakeholders associated with the agreed upon process areas.
  - Facilitate discussions and to gain an understanding of the current state processes and internal controls, personnel involved, and supporting technology.
- **Document Current State Processes and Internal Controls**
  - Document the current state processes and internal controls, as necessary, to mitigate relevant risks as defined by the discussion.
  - Identify flow of a process, various internal control points that exist within each process, and identify significant risks.

Impact on Controls, cont'd

- **Walkthrough of Processes, Internal Controls and Supporting Documentation**
  - A walkthrough is the method of discussing all relevant processes and internal controls with key stakeholders and observing and/or inspecting the documentation available to validate whether appropriate documentation appears to be in place.

Outcomes and Improvements

- Outcomes include
  - Determine if current internal controls are designed appropriately to mitigate the identified risks.
  - Determine adequacy of the design of internal controls that currently exist as it relates to effective and efficient achievement of the specified purpose.
  - Provide detailed recommendations for future state improvements to internal controls.
  - Identify inefficient and ineffective processes and departures from existing policies and procedures — assess current management processes to identify issues and their underlying cause (i.e. people, process, or technology).

Prioritize Risks and Develop Audit Plan

- Primary methods to select audits to include in audit plan:
  - Cycle/Rotation Approach
  - Risk Based Approach (most popular)

Benefits of Risk Based Audit Planning

- Efficient use of resources
- Improves ability to impact organization
- Generates buy-in from management
- Creates ***value***

Prioritize Risks and Develop Audit Plan, cont'd

- Map risks to audits
- Rank the audits
- Audit plan based on coverage of total risk

Risk Assessment Results

- Results should be reviewed and challenged (peer review)
- Results should drive frequency and intensity of audit coverage
- Assurance can be provided through multiple delivery channels e.g. end-to-end process reviews, targeted procedures

Communicating Results

- Present an overview of the risk assessment process by highlighting the key steps followed in the three phases
  - Phase One: Develop Audit Universe
  - Phase Two: Identify and Analyze Risks
  - Phase Three: Weigh and Score Risks
- Develop a summary of the most significant risks
  - Categorize risks into financial, operational, and compliance

Communicating Results to Audit Committee

- Consider using a heat map

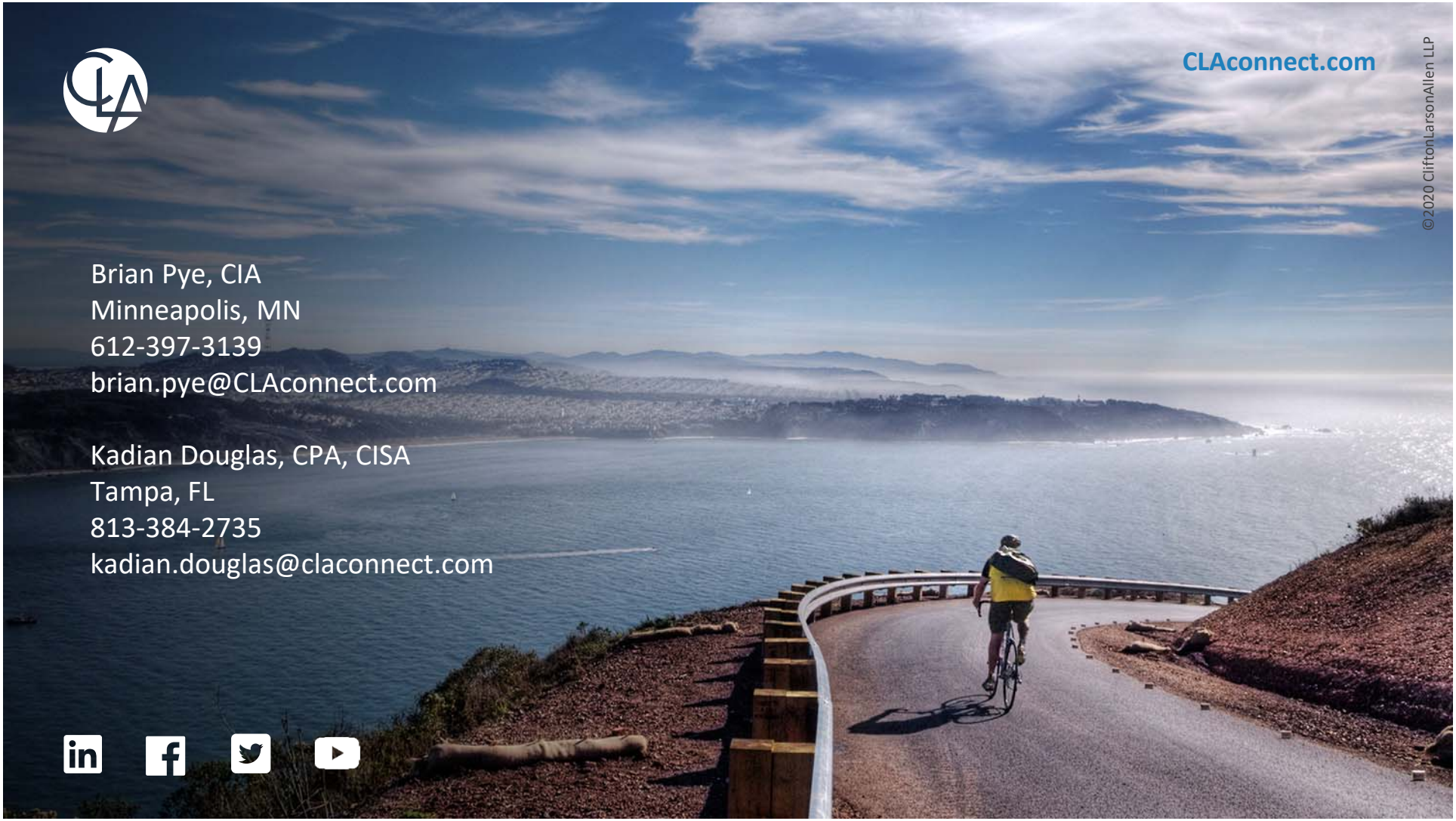
- Understand reader's expectations (high, medium and/or low reporting)

Best Practices

- Get consensus on measuring risks and risk tolerances
- Establish participants' understanding of the effectiveness of controls and other risk responses used in the institution
- Work closely with leadership to understand strategy and key objectives
- Communicate a high level clear summary of the Risk Assessment with the Audit Committee

Key Takeaways

- GLBA will be tested as part of the student financial aid audit
- GLBA requirements tested could increase in the future
- Risk Assessment is not an annual, one-time event
- Risk assessment considerations will differ based on the level of assessment
- Risk Assessment is more than simple risk identification – must include robust analysis
- Requires continuous engagement with relevant stakeholders
- Full written explanation of the Audit Plan and thought process applied
- Risk Assessment must be integrated into audit execution
- Common risk definitions support risk “convergence” with other lines of defense


CLAconnect.com
©2020 CliftonLarsonAllen LLP
Brian Pye, CIA
Minneapolis, MN
612-397-3139
brian.pye@CLAconnect.com
Kadian Douglas, CPA, CISA
Tampa, FL
813-384-2735
kadian.douglas@claconnect.com