HOW TO PREPARE FOR AND ACE YOUR GLBA AUDIT

500 Federal Street
Suite 540
Troy, NY 12180
www.greycastlesecurity.com
(800) 403-8350
PRESENTER

Stan Letarte
Security Strategist
GreyCastle Security
<table>
<thead>
<tr>
<th>UNDERSTANDING YOUR OBLIGATION</th>
<th>WHAT WILL BE AUDITED</th>
<th>EVIDENCE OF COMPLIANCE</th>
</tr>
</thead>
</table>

UNDERSTANDING THE OBLIGATION
GRAHAM-LEACH BLILEY ACT

GLBA went into effect in May, 2002, with compliance required by May of 2003. The Federal Trade Commission (FTC) has authority for regulating Higher Education’s compliance to the law.

GLBA consists of:
- the Pretexting Rule
- the Privacy Rule
- the Safeguards Rule

GLBA applies to education institutions because of their involvement in financial activities that are defined in banking laws; the 2015 Title IV Program Participation Agreement (PPA) signed you up for this compliance.

Image Credit: https://cdn.pixabay.com/photo/2017/01/18/22/06/law-1991004_960_720.jpg
With respect to the *Privacy Rule* the FTC specifically states that:

“Any institution of higher education that complies with the Federal Educational Rights and Privacy Act ("FERPA")\(^1\) and its implementing regulations\(^2\) and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA”\(^3\).

---

1. [https://www.law.cornell.edu/uscode/text/20/1232g](https://www.law.cornell.edu/uscode/text/20/1232g)
2. [https://www.law.cornell.edu/cfr/text/34/part-99](https://www.law.cornell.edu/cfr/text/34/part-99)
3. [https://www.law.cornell.edu/cfr/text/16/313.1](https://www.law.cornell.edu/cfr/text/16/313.1)
Complying with the Safeguards Rule has three objectives:

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of that customer data
- Protect against unauthorized access to or use of customer data, which could result in substantial harm or inconvenience to customers

In order to do this, the FTC mandates that Educational Institutions:

“... develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the institution's] size and complexity, the nature and scope of [institutional] activities, and the sensitivity of any customer information at issue”¹

¹ [https://www.law.cornell.edu/cfr/text/16/314.3](https://www.law.cornell.edu/cfr/text/16/314.3)
WHAT THE AUDIT COVERS

In July of 2019, the FTC came out with audit objectives that were added to the federal common audit\textsuperscript{1,2}. The audit objectives are not aimed at the content of the security program but are more simplistic in this version of the audit. Paraphrased, these objectives are:

- The institution has named someone to coordinate its information security program.
- It has conducted a risk assessment covering employee training and management, networks and information systems, and incident response.
- It has implemented safeguards to address the identified risks in those areas.

\textsuperscript{2} See also: \url{https://www2.ed.gov/about/offices/list/oig/nonfed/cpa1901.pdf}
GUIDE TO MORE THAN SURVIVAL
GLBA OBLIGATIONS EXCEED AUDIT

16 CFR 314.4¹ – *Elements* specifies five actions for the security program:

1. Designate an employee or employees to coordinate the institution's information security program
2. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, etc.
3. Design and implement information safeguards to control the risks that the institution identifies through risk assessment and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures
4. Oversee service providers
5. Adjust the institution's information security program considering the results of security assessment

¹ [https://www.law.cornell.edu/cfr/text/16/314.4](https://www.law.cornell.edu/cfr/text/16/314.4)
ACCOUNTABILITY FOR THE PROGRAM

**Required:** “the institution appoint an employee or employees specifically to oversee the Information Security Program”

Unlike many security regulations, GLBA does not require a CISO, but merely “an employee or employees”

**Warning:** the employee(s) chartered to oversee this program must have:

- An understanding of the business, security and the law, and;
- Sufficient time to apply to managing the program
**RISK ASSESSMENT**

**Required:** “identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information; it must then assess the sufficiency of any safeguards in place to control these risks.”

- Determine your vulnerabilities (suggestion: use a control framework such as NIST 800-171 or NIST 800-53)
- Understand threats that might exploit those vulnerabilities
- Hire a professional assessor that can dive deep but explain in a manner that is business-relevant.
- Create a roadmap for action (i.e. which safeguards will you apply?)
INFORMATION SAFEGUARDS

**Required:** “design and implement information safeguards to control the risks that the institution identifies through risk assessment and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures”

- GLBA specifically calls out Administrative, Technical and Physical Safeguards: this is not purely a technical/IT effort!
- NIST 800-53 and NIST 800-171 are both recommended control frameworks for Higher Education (see resources section)
- The free guide for this Webinar provides a template to organize your security controls
OVERSEE SERVICE PROVIDERS

**Required:** “any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.” (16 CFR, section 314.2)

Section 314.4 requires that Service Providers:

1) Be selected through reasonable steps to assure that they can maintain the appropriate safeguards

2) Are contracted in a manner that forces maintenance of the safeguards
MAINTAIN THE INFORMATION SECURITY PROGRAM

Lastly, section 314.4 requires that you:

“Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program”

Generally speaking, this means that you need to assess security regularly and review & adjust your Information Security Program whenever needed, due to:

• Newfound vulnerabilities
• Planned or unplanned changes to your environment
• Changes in threats
SURVIVING
THE AUDIT
DOCUMENTATION: A KEY

• Written security program
• Accountability for implementing the program – consider a “charter” statement from Cabinet-level staff
• Risk Assessment – if you have no experience with assessing Cyber-risk, hire a firm to do this! The assessment should follow generally-accepted procedures for risk assessment and must have a formal, written report for you to show the auditors
• Safeguards – for those risks called out in the assessment, document your administrative, technical and physical controls that will address the risks
## GLBA Security Requirements Worksheet

<table>
<thead>
<tr>
<th>GLBA Safeguards Requirements</th>
<th>College Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>§314.3 Standards for safeguarding customer information.</strong></td>
<td><strong>Activity Description</strong></td>
</tr>
</tbody>
</table>
| **Information security program.** You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and that includes technical and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the level of risk associated with your business operations. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section. | Addressed via:  
- Policy and Standards Manual  
- Development and Acceptance of Information Security Policy  
- PCI ASS 1.1 | Year 3  
- Complete  
- Q4 2018 |
| **Objectives:** The objectives of section 501(b) of the Act, and of this part, are to | **Status** |
| (1) Insure the security and confidentiality of customer information; | Addressed via:  
- Risk Assessment (GCS)  
- Vulnerability scanning  
- Development and Acceptance of Information Security Policy  
- Development and Acceptance of Data Classification Policy and Procedure  
- PCI Assessment | **Complete**  
- Ongoing  
- Complete  
- Complete  
- Q4 2018 |
| (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and | | |
YOU HAVE TO COMPLY WITH GLBA

GLBA IS VAGUE, BUT EXPANSIVE IN SCOPE

COMMON FEDERAL AUDIT WILL COVER A SUBSET OF GLBA
QUESTIONS?

@greycastlesec
(800) 403-8350
www.greycastlesecurity.com
ADDITIONAL RESOURCES

- Educause article regarding the audit objectives: https://er.educause.edu/blogs/2019/7/the-safeguards-rule-audit-objective-is-here