**Responses to Questions at January 26, 2023 Webinar**

In the CACUBO Webinar on GLBA, there were various questions asked for which the speakers did not get a chance to respond to due to time. The following are those questions and responses from RSM, the presenters. Please keep in mind that the responses provided herein are the views and thoughts of the presenters. Please consult with you own external accounting firm for the response that might be most pertinent to your institution.

**Question 1**

I'm curious - can the InfoSec officer technically be the SOC?

**RSM Response:**

If I’m understanding the question, the Security Operations Center cannot function as the InfoSec Officer.  It must be a ‘single’ qualified individual.  That said, the leader from the SOC could (feasibly) act in this role provided they are “qualified” and it’s a single individual.

**Question 2**

Are there recommendations for "monitoring" a small local vendor that may not be on the HECVET list?

**RSM Response:**

You can download the HECVAT and send it to them to respond to you.  Then you can evaluate their response and periodically audit them using the HECVAT Form.

<https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit>

Ultimately, the Safeguard Rule encourages a risk-based approach to identify service providers that handle sensitive student financial data. For the Safeguard rule, it’s best to evaluate the ‘relationship’ versus the size of the provider.  You may have a small vendor, but the amount of sensitive data shared with the third-party may be significant.  In the event we share a significant amount of sensitive data, the relationship would be significant and should be evaluated to ensure the service provider has implemented controls in alignment with the Safeguard Rule.  Contact Bob Eckmann at [Bob.Eckman@RSMUS.com](mailto:Bob.Eckman@RSMUS.com) for more or for assistance with implementing HECVAT, 3rd party review processes.

**Question 3**

So in your professional opinion should GLBA coordinator NOT be in IT?

**RSM Response:**

Yes – Professional opinion that the GLBA coordinator should NOT be in IT.  There are a few factors to consider:

1. The intent of the Final Rule is to designate a ‘single’ and ‘qualified’ individual responsible for the information security program.
2. The final rule exempts organizations with less than 5,000 consumers.
3. Higher Education on average costs ~$35,000. This would indicate that the university could manage as much as 175 million in revenue before being large enough to comply with the rule.
4. Per the FTC’s clarification to questions related to the Final Rule, “financial institutions may designate any qualified individual who is appropriate for their business. Only if the complexity or size of their information systems require the services of an expert will the financial institution need to hire such an individual.”
5. In most cases, universities with more than 5,000 students have complex IT infrastructures that warrant a designated expert.
6. Finally, the intent of the rule is to assign accountability. Per paragraph (d) of the new rule, management should ensure a process is established to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.  We recommend testing is performed by independent parties.

In short, the GLBA Coordinator should reside within whichever department is most responsible for the confidentiality, integrity, and availability of SFA related data.  This determination should be made “absent” of any reporting structure.    There is nuance on reporting when a service provider or an affiliate is used to cover this responsibility, but the new rule does not specify where an internal designated qualified individual must be independent of IT.

Contact Bob at [Bob.Eckman@RSMUS.com](mailto:Bob.Eckman@RSMUS.com) or [John.MacDonald@rsmus.com](mailto:John.MacDonald@rsmus.com) for more or for assistance with determining how to best position the GLBA coordinator.

**Question 4**

Can you provide documentation regarding the requirement that the security person not be a member of IT?

**RSM Response:**

Refer to response above to Bryan Howard.

**Question 5**

Can I have a direct reference for the "independence" requirement for the qualified individual responsible for the program under GLBA safeguard rules? There is nuance on reporting when a service provider or an affiliate is used to cover this responsibility, but I do not see where an internal designated qualified individual has their reporting specified.

**RSM Response:**

Refer to response above to Bryan Howard.

**Question 6**

Do we know if auditors have been given the tools needed to determine compliance?

**RSM Response:**

From my experience they are using a myriad of tools to determine compliance.  Most have created their own tool(s) (typically spreadsheets) to evaluate programs.  The DOE recommends utilization of the NIST 800.171 to evaluate  the best coverage for security controls, but we’d suggest that you cross walk the GLBA controls and focus on those as it pertains to SFA Applications, infrastructure, and data.

Contact Bob at [Bob.Eckman@RSMUS.com](mailto:Bob.Eckman@RSMUS.com) or [John.MacDonald@rsmus.com](mailto:John.MacDonald@rsmus.com) for more or for assistance with determining the best methods for GLBA program evaluation.

**Question 7**

Is there a clear distinction on what encryption at rest is (for example - drive level vs file level or if in a database at the column level, etc.)?

**RSM Response:**

Fortunately or unfortunately the rule does not distinguish.  It states “encrypted” provide you’re using an industry standard (such as AES 256 or better) there doesn’t appear to be any distinction between drive, file, database, tuple, or field level encryption.   In other words, you’re allowed to use your discretion and available toolsets for this requirement.  I’d suggest this be addressed as part of your Data Management / Governance program.

Contact Bob at [Bob.Eckman@RSMUS.com](mailto:Bob.Eckman@RSMUS.com) or [John.MacDonald@rsmus.com](mailto:John.MacDonald@rsmus.com) for more help with determining

**Question 8**

How do they define customer data "at rest"

**RSM Response:**

Technically, Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way.  (consider physical information such as paper as well!)  Per the Safeguards Rule, “Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual.” (Source = [eCFR :: 16 CFR 314.4 -- Elements.](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4) (c) 3.)

**Question 9**

Is there a data dictionary somewhere that specifically shows what data elements are considered as "SFA Data?"  All data is not SFA, so what data is the FTC specifically wanting to safeguard?  The scope of the data has always been a question for me.

**RSM Response:**

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.  <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

Non-Directory (eg. unsearchable on Google). This rule covers most personal information (name, date of birth, Social Security number) as well as transactional data (card numbers), account numbers, or other information used to secure a loan.  The rule provides an import explanation to consider.  Generally, a students name is consider public data; however, a student’s affiliation with the university is not considered public. As such, a student name linked to the university would be considered GLBA data.

**Question 10**

This was an excellent (and slightly scary) presentation. I would love to have the copy of the recording to share with our IT department! Thank you!

**RSM Response:**

Marty will be posting the recorded presentation.  We are happy to connect with your IT department and provide additional background on your behalf as well.

**Question 11**

You say within 24 hours, but I believe it says "immediately. Can you give us the reference for 24 hours?

**RSM Response:**  This is copied from the SAIG agreement, “The Agency will report to the Department in writing any use, disclosure, or re-disclosure of ISIR data or FAFSA Filing Status Information not authorized by this Agreement. The Agency shall submit the report **within one (1) business day** after the Agency learns of such unauthorized use, disclosure, or redisclosure to: U.S. Department of Education, Federal Student Aid, 830 First St. NE., Union Center Plaza, Room 32E1, Washington, DC 20202 or via e-mail at [FAFSACompletion@ed.gov](mailto:FAFSACompletion@ed.gov). The report must identify:

1. The nature of the unauthorized use, disclosure, or re-disclosure;
2. The ISIR data or FAFSA Filing Status Information used, disclosed, or re-disclosed;
3. The person or entity, if known, who made the unauthorized use or received the unauthorized disclosure, or re-disclosure;
4. What the Agency has done or will do to notify affected FAFSA applicants and to mitigate any deleterious effect of the unauthorized use, disclosure, or re-disclosure;
5. What corrective action the Agency has taken or will take to prevent future similar unauthorized use, disclosure, or re-disclosure.”

I think it is also important to note that you have some discretion related to when “the clock starts” for reporting.  It is suggested that you have a “Safeguards Committee” established who, when then CSIRT determines that SFA may be involved in the breach, would risk assess and determine when/if the clock needs to start.  Document your approach.  It is my experience that regulators are more understanding of a good faith effort that incorporates industry reasonable standards, than an approach that simply ignores the requirements.

Contact Bob at [Bob.Eckman@RSMUS.com](mailto:Bob.Eckman@RSMUS.com) or [John.MacDonald@rsmus.com](mailto:John.MacDonald@rsmus.com) for more or for assistance with this question.