INFORMATION TECHNOLOGY UPDATE

Information Technology Internal Control Testing

While using the new Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool *is* "optional," what *isn't* optional is a lack of cybersecurity which could lead to a Gramm-Leach-Bliley Act breach. When evaluating internal controls, financial institutions must consider both the Cybersecurity Assessment Tool (CAT Tool) and the Gramm-Leach-Bliley Act (GLBA). The CAT Tool and GLBA require a detailed discussion of existing controls in conjunction with an annual assessment of whether these controls effectively mitigate risk.

In 2016, the FFIEC implemented the CAT Tool to reduce the risk of cybersecurity attacks and determine a financial institution's security posture. With over 100 questions related to various existing security controls, the CAT Tool allows financial institutions to grade their overall security posture via simple yes or no answers. While implementing the tool appears straightforward, what isn't painless is collecting the supporting documentation and control testing to ensure these controls are actually in place and effective. If weaknesses exist, institutions could pinpoint them before regulators do.

Regulators also seek approval of financial institutions' adherence to the GLBA requirements. Financial institutions must perform a detailed information security risk assessment that is updated and approved annually by the Board of Directors. Before evaluating the competency of the controls in place, the financial institution should detail the initial risk ratings, which consider the probability of an event as well as its potential impact on the institution in the absence of controls. After determining its risk profile, the financial institution should describe all preventative controls, which reduce the probability of an event, as well as detective and corrective controls, which reduce the impact of an event. Internal control testing is then performed to assess the controls' true risk mitigating effectiveness. Lastly, the financial institution should assign a residual risk rating based on the results of testing and the controls' perceived effectiveness, from which the financial institution will determine whether the remaining risk is acceptable or further controls are necessary.

Providing documentation that adheres to both the GLBA and CAT Tool requirements is a daunting task for any financial institution. However, with the help of advanced internal information technology audits, institutions can alleviate that daunting task. S.R. Snodgrass IT audits cover **all** CAT Tool questions and GLBA compliance controls and map those controls to the work papers. As a result, regulators can easily cross-reference testing results with the reported controls. Plus, any weaknesses will have already been disclosed, and possibly remediated, before the regulators arrive.

If you have any questions regarding this Update, please feel free to contact Jeremy Burris, Rob Haller, or Chris Kreutzer at (724) 934-0344 or (800) 580-7738, or email jburris@srsnodgrass.com, rhaller@srsnodgrass.com, or ckreutzer@srsnodgrass.com.

2009 Mackenzie Way, Suite 340 Cranberry Twp., PA 16066 | Phone (724) 934-0344 | Fax (724) 934-0345 | Email: info@srsnodgrass.com
1275 Glenlivet Drive, Suite 135 Allentown, PA 18106 | Phone (610) 530-8885 | Fax (610) 530-0409
2100 Renaissance Blvd., Suite 110 King of Prussia, PA 19406 | Phone (610) 278-9800