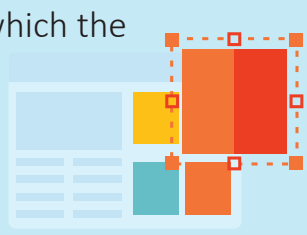
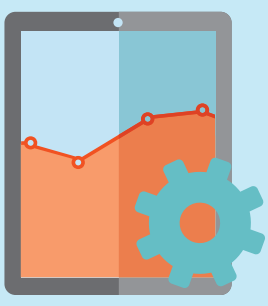
QUESTION:
If I complete the FFIEC Cybersecurity Assessment, does my financial institution still need to perform an annual IT Risk Assessment?

ANSWER:
Yes. Completion of the FFIEC Cybersecurity Assessment does not replace the need for an annual IT/Information Security (IS) Risk Assessment. The following outlines some of the differences between an IT Risk Assessment and the FFIEC Cybersecurity Assessment.

IT Risk Assessment	FFIEC Cybersecurity Assessment
FOCUS	
IT/IS Risk Assessments are detailed, customized assessments that evaluate the status of your financial institution's security program. The controls and threats that are examined during the assessment are specific to your financial institution's unique IT environment. 	The Cybersecurity Assessment measures all financial institutions against the same set of metrics and standards. The Cybersecurity Assessment is not customized to evaluate your financial institution's unique IT security program. Instead, it measures your financial institution's maturity levels according to the NIST Cybersecurity Framework. 
CYBERSECURITY MODELS	
Although TraceSecurity's IT/IS Risk Assessment is based on the NIST Cybersecurity Framework, the NIST Framework is only one of many sets of security standards and best practices from which IT Risk Assessments can be modeled. 	The Cybersecurity Assessment was built from, and directly maps to, the NIST Cybersecurity Framework. It does not measure a financial institution's maturity levels against any other set of standards or security best practices. 
THREATS	
IT/IS Risk Assessments identify the threats to your financial institution's assets as well as the impact and probability of those threats occurring within your individual IT environment. 	The Cybersecurity Assessment establishes a high-level overview of your financial institution's inherent risk level but does not consider specific threats to your financial institution. 
CONTROLS	
IT/IS Risk Assessments evaluate not only the existence of security controls but also the effectiveness of the controls used to mitigate threats to your IT security program. 	The Cybersecurity Assessment does not evaluate the effectiveness of your financial institution's security controls. Rather, it evaluates the extent to which the NIST Cybersecurity Framework has been implemented in your financial institution based on the security processes or controls that exist in your financial institution. 
TYPES OF RISKS	
IT/IS Risk Assessments examine your financial institution's residual risk – the risk level that remains after your financial institution implements controls to combat the threats to your IT environment. 	Residual risk is not considered when conducting the Cybersecurity Assessment. The tool assesses the risks to your financial institution without considering the effect of the security controls used to mitigate those risks. 
COMPLIANCE	
Financial institutions are required to conduct an IT/IS Risk Assessment on an annual basis. 	At this time, the FFIEC does not require financial institutions to complete the Cybersecurity Assessment; however, it is strongly encouraged as an ongoing business practice. 

PROACTIVELY COMBAT AGAINST CYBERSECURITY RISK

To address increasing security threats and evolving regulatory guidelines, your financial institution should incorporate both the FFIEC Cybersecurity Assessment and an annual IT Risk Assessment into your ongoing risk management program.

Doing so will help ensure your ability to continuously evaluate and monitor your cybersecurity posture as well as maintain compliance with regulatory guidance.

tracesecurity
GRC Simplified... Finally.

6300 Corporate Blvd, Suite 200
Baton Rouge, LA 70809

info@tracesecurity.com
www.tracesecurity.com