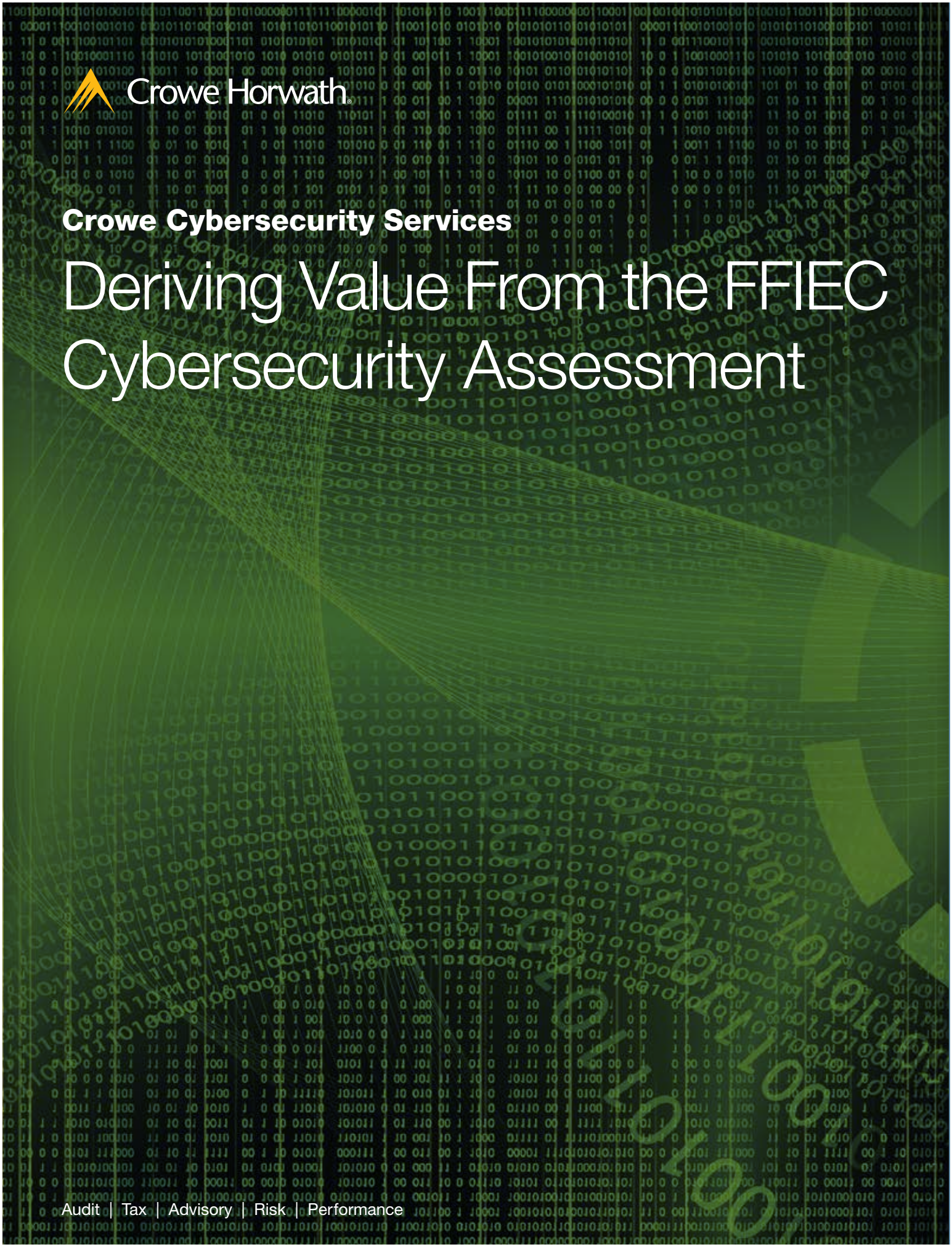

Crowe Horwath
Crowe Cybersecurity Services
Deriving Value From the FFIEC Cybersecurity Assessment
Audit | Tax | Advisory | Risk | Performance

The Cybersecurity Assessment Tool developed by the Federal Financial Institutions Examination Council (FFIEC) can help financial institutions identify risks and evaluate their cybersecurity maturity. But many organizations encounter questions and challenges related to the tool. Crowe Horwath can help financial institutions address these concerns and derive greater value from this important new tool.

Getting the Most From a Valuable Tool

The FFIEC Cybersecurity Assessment Tool (Exhibit 1) is designed to provide banks and other financial institutions with a repeatable and measurable process for assessing their cybersecurity preparedness. It also provides valuable insights into regulators' priorities and expectations about the critical issue of cybersecurity risk management practices and controls.

As useful as the FFIEC Cybersecurity Assessment Tool is, however, it also has raised some questions and concerns among financial institutions, such as:

- How critical is it that we use this tool? Will regulators expect to see it used extensively?
- How does this new tool relate to other existing cybersecurity guidance such as the National Institute of Standards and Technology (NIST) framework and the Payment Card Industry (PCI) Data Security Standards?
- How can we efficiently and accurately gather all of the information that is needed to answer the tool's inherent risk assessment questions?
- How should we evaluate the many unique controls identified in the tool to determine which are most practical and appropriate for our institution?
- How can our information security team apply the tool most efficiently, given our existing resources and competing priorities?
- What steps should we take to maintain objectivity and accuracy in our self-assessments?

Crowe cybersecurity specialists have extensive experience in helping institutions address these concerns in order to apply the FFIEC Cybersecurity Assessment Tool in a way that derives the greatest potential benefit from this important new tool.

The Crowe Perspective – Maturity Plus Effectiveness

Altogether, the FFIEC Cybersecurity Assessment Tool identifies nearly 500 distinct cybersecurity controls. The controls are highly prescriptive, and increased maturity is accompanied with additional control expectations within the tool. This approach is appropriate as part of a regulatory approach, but it differs slightly from the definition of maturity used in other frameworks such as the NIST standard.

More important, when evaluating the effectiveness of a cybersecurity control environment, institutions need to understand whether their cybersecurity controls are:

- Effectively mitigating the risk they are designed to manage
- Operating efficiently to provide maximum value to the institution
- Designed to enable the institution to effectively respond to a security incident or other external influencer

Drawing on decades of experience in the financial services industry, as well as direct expertise in information technology and cybersecurity issues, Crowe cybersecurity specialists can help financial institutions go beyond the focus on control effectiveness, and focus instead on a broader and more crucial objective: leveraging the FFIEC cybersecurity guidance to implement a cybersecurity control framework that is effective, efficient, and responsive.

The Crowe Approach – Broad-Based and Proactive

In addition to applying the components of the FFIEC tool, Crowe cybersecurity teams can help financial institutions develop a more comprehensive methodology to help implement a more effective and proactive long-term cybersecurity initiative.

Key components of the Crowe approach include:

- **FFIEC Cybersecurity Gap Assessment** – Crowe teams perform an assessment against the FFIEC framework or can evaluate an institution's own self-assessment, including both the inherent risk assessment and the cybersecurity control assessment.
- **Cybersecurity Maturity Assessment** – Crowe teams evaluate the effectiveness, efficiency, and responsiveness of the control environment to determine the current maturity level. Crowe can incorporate expectations from the FFIEC Cybersecurity Assessment Tool, NIST, or any other framework based on the client's needs.
- **Cybersecurity Road Map** – Building on the results of the gap or maturity assessment, Crowe teams can work directly with banks' cybersecurity teams to identify long-term goals that anticipate future threats and concerns. With the desired future state defined, Crowe implementation teams can help plan, develop, and implement specific initiatives to support the long-term cybersecurity strategy.

The Crowe approach is flexible, scalable, and responsive, so that financial institutions can customize their cybersecurity initiatives in a way that provides the depth and breadth of service that is most appropriate to their situation.

The Crowe Benefit to Client – Industry and Technical Expertise

Like any tool, the FFIEC Cybersecurity Assessment Tool provides the greatest value in the hands of experienced users who understand how to apply it effectively. The cybersecurity specialists at Crowe have extensive experience in developing, implementing, and applying security frameworks in various environments. They also can offer deep insights into financial industry best practices that have been applied successfully in other institutions.

This combination of technical and industry expertise brings added value to client organizations and ultimately enables financial institutions to strengthen their own information security capabilities, paving the way for a proactive approach toward achieving and maintaining the desired level of cybersecurity maturity.

FFIEC Cybersecurity Assessment Tool at a Glance

Released in 2015, the FFIEC Cybersecurity Assessment Tool consists of two parts:

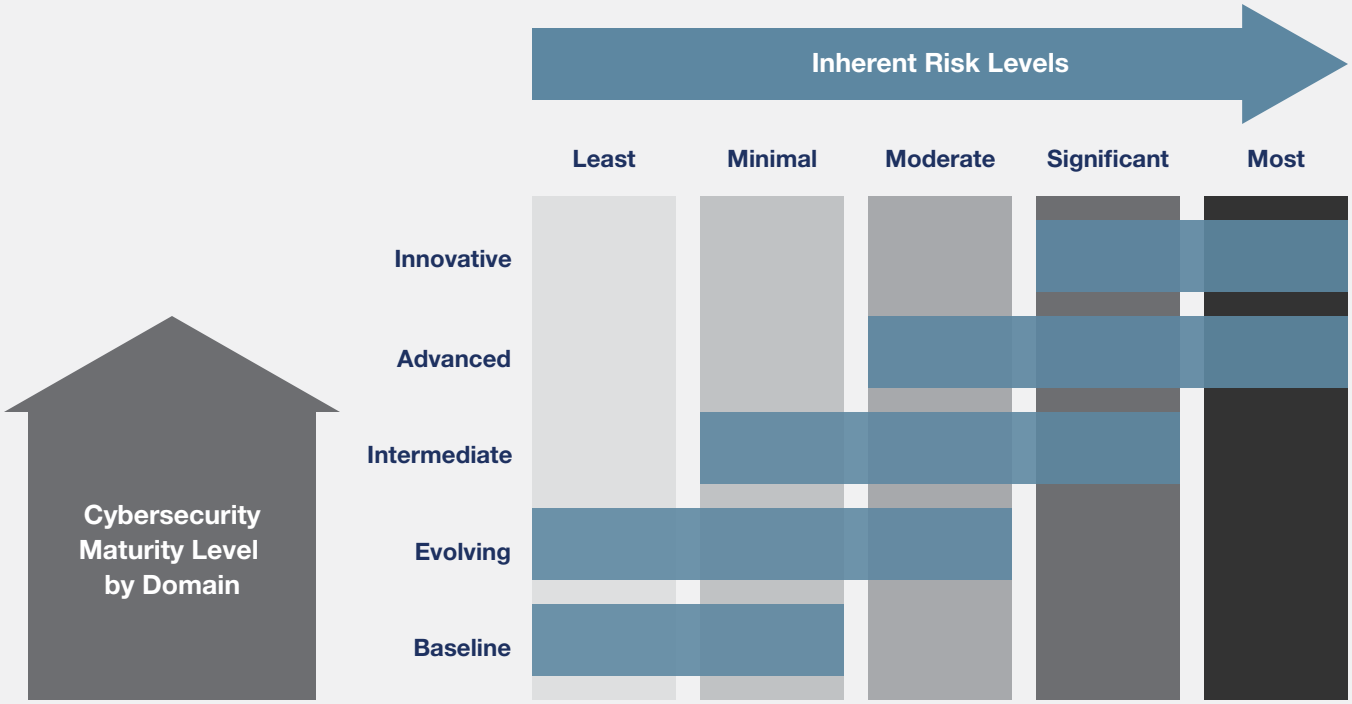
1. **Inherent Risk Profile** – identifies the level of risk posed to the institution by:
   - Technologies and connection types
   - Delivery channels
   - Online/mobile products and technology services
   - Organizational characteristics
   - External threats
2. **Cybersecurity Maturity** – measures the institution's level of risk and controls across five domains:
   - Cyber risk management and oversight
   - Threat intelligence and collaboration
   - Cybersecurity controls
   - External dependency management
   - Cyber incident management and resilience

The results of the inherent risk profile define the level of controls that would be expected to be in place. The two parts are then aligned to determine the institution's risk/maturity relationship in each domain. The expected cybersecurity maturity level is based on the inherent risk level of the institution.

Regulators have said that use of the cybersecurity assessment is voluntary – yet examiners are being trained in the FFIEC Cybersecurity Assessment Tool and have begun asking for institutions' self-assessment results in advance of examinations. Financial institutions can expect more awareness and sensitivity to cybersecurity controls from their examiners, and should be prepared to demonstrate a mature understanding of cybersecurity tools within the context of the FFIEC assessment.

Crowe Horwath

Exhibit 1: FFIEC Cybersecurity Assessment Tool



Contact Information

For more information on Crowe cybersecurity services, please contact:

Raj Chaudhary
+1 312 899 7008
raj.chaudhary@crowehorwath.com

Mike Del Giudice
+1 630 575 4359
mike.delgiudice@crowehorwath.com

About Us

Crowe Horwath LLP (www.crowehorwath.com) is one of the largest public accounting, consulting, and technology firms in the United States. Under its core purpose of "Building Value with Values,®" Crowe uses its deep industry expertise to provide audit services to public and private entities while also helping clients reach their goals with tax, advisory, risk and performance services. With offices coast to coast and 3,000 personnel, Crowe is recognized by many organizations as one of the country's best places to work. Crowe serves clients worldwide as an independent member of Crowe Horwath International, one of the largest global accounting networks in the world. The network consists of more than 200 independent accounting and advisory services firms in more than 120 countries around the world.

www.crowehorwath.com

MOHAWK windpower

When printed by Crowe Horwath LLP, this piece is printed on Mohawk Color Copy Premium, which is manufactured entirely with Green-e® certified wind-generated electricity.