Understanding the FFIEC Cybersecurity Assessment Tool: An Internal Audit Perspective
Introduction

"IT IS ONLY A MATTER OF WHEN BEFORE SOMEONE USES CYBER AS A TOOL TO DO DAMAGE TO CRITICAL INFRASTRUCTURE WITHIN OUR NATION."

– Adm. Michael Rogers, U.S. National Security Agency Director

Tick, tock, tick, tock… Admiral Rogers’s warning is chilling: A major cyberattack against U.S. critical infrastructure is simply a matter of time. Cybersecurity risk management has been a top priority for financial institutions, their boards of directors and their regulators for some time. In June 2015, the Federal Financial Institutions Examination Council (FFIEC) released the cybersecurity assessment tool (the Assessment) to help financial institutions identify their cyber risks and determine their cybersecurity maturity and preparedness. The assessment tool will be used during federal agency examinations with the intent of collecting data across industry peers for the purposes of benchmarking and to support examination conclusions.

The FFIEC Assessment was designed to complement the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security, released in February 2014. Since its release, the NIST framework has quickly become the U.S. standard for institutions aiming to assess their cybersecurity maturity and reduce risk to their critical infrastructure. The FFIEC Assessment supplements the popular NIST framework with guidance specific to federally supervised financial institutions.

The Assessment was the result of work performed by the Cybersecurity and Critical Infrastructure Working Group (CCWIG) from June 2013 through the date of issuance, June 30, 2015. The CCWIG was comprised of a number of government agencies from intelligence, law enforcement and Homeland Security. NIST representatives reviewed and provided input on the mapping of the Assessment to the NIST cybersecurity framework – an exercise designed to ensure consistency between these two resources. Both NIST and the Assessment share principles and concepts that appear in earlier forms of cybersecurity guidance (e.g., ISO, COBIT, Council on Cybersecurity [CCS], Center for Internet Security Critical Security Controls [CSC]), thus ensuring continuity in the direction of cybersecurity efforts.

Since the FFIEC Assessment is positioned to become the de facto method of conducting enterprise cybersecurity assessments for federally supervised financial institutions, internal audit departments and functions need to be familiar with the tool and the way it works and understand their role in applying it to the enterprise. Internal audit’s responsibilities include an independent validation of the assessment process performed by management, which itself consists of two parts – an inherent risk profile and a cybersecurity maturity assessment. These topics, along with a brief look at the current state of cybersecurity, are covered in this white paper.

FFIEC’s Cybersecurity Priorities

The FFIEC’s recent research, including its 2014 evaluation of cyber-risk preparedness among more than 500 financial institutions, helped produce seven cybersecurity priorities for 2015. The same priorities also will guide the council’s work in 2016:

2. Incident Analysis: FFIEC members will enhance its processes for gathering, analyzing and sharing information with each other during cyber incidents.
3. Crisis Management: FFIEC will align, update and test emergency protocols to respond to system-wide cyber incidents in coordination with public-private partnerships.
4. Training: FFIEC will develop training programs for its members on evolving cyber threats and vulnerabilities.
5. Policy Development: FFIEC will update and supplement its Information Technology Examination Handbook to reflect rapidly evolving cyber threats and vulnerabilities with a focus on risk management and oversight, threat intelligence and collaboration, cyber security controls, external dependency management, and incident management and resilience.
6. Technology Service Provider Strategy: FFIEC’s member agencies will expand their focus on technology service providers’ ability to respond to growing cyber threats and vulnerabilities.
7. Collaboration With Law Enforcement and Intelligence Agencies: The Council will build upon existing relationships with law enforcement and intelligence agencies to share information on the growing cybersecurity threats and response techniques.

STATE OF CYBERSECURITY AND THE NEED FOR THE ASSESSMENT

Conducting assessments using the FFIEC tool requires some context regarding the current state of cybersecurity. Cybersecurity discussions take place with greater frequency throughout enterprises today, from the boardroom and C-suite, to IT, legal, finance and more. Asset management processes and third-party vendor management programs represent two notable areas of cybersecurity in need of improvement. Many companies don’t know what information assets they have, where they are located and what data resides on them, which prevents them from establishing a solid foundation for their cybersecurity efforts—a company can’t protect what it doesn’t know it has. Not all assets require equal levels of protection; determining which ones are important (“crown jewels”) is necessary in order to assign the proper level of risk and protection. Gaining the knowledge to make that determination, however, can be a challenge. Complex IT environments and the pervasive nature of unsanctioned software and hardware (also known as “shadow IT” and often propagated by Bring Your Own Device [BYOD] policies) make the job of keeping track of and maintaining security across devices extremely difficult. Finally, the cybersecurity components of many third-party vendor management programs have failed to keep pace with the increased volume and complexity of outsourced services.

While companies are intent on fortifying their cyber walls, the following remarks made by FFIEC agencies further support the use of the assessment tool as they indicate the agencies will be using the FFIEC assessment tool in conducting examinations of financial institutions in 2016:

- The Federal Reserve Board has explicitly stated its intent to begin using the Assessment, “…in late 2015 or early 2016 … as part of [the] examination process when evaluating financial institutions’ cybersecurity preparedness in information technology and safety and soundness examinations and inspections.”

---

• The FDIC has indicated, through Financial Institution Letter 28-2015, that “FDIC examiners will discuss the Cybersecurity Assessment Tool with institution management during examinations to ensure awareness and assist with answers to any questions.”

• A senior OCC official remarked that “the use of the assessment tool is optional for financial institutions; however, OCC examiners will use it to supplement exam work to gain a more complete understanding of an institution’s inherent risk, risk management practices, and controls related to cybersecurity. While we will never really know if these measures actually thwart a specific attack, we can be certain that more breaches will occur if we do not commit to being vigilant and continuously enhancing our ability to prevent, detect, and recover from cyber incidents.”

Furthermore, the FFIEC outlines specific responsibilities for the board and the chief executive officer (CEO) in implementing the Assessment, listed below:

### The Role of the Board and CEO in Implementing the Assessment

#### The Board
- Engages management in establishing the institution’s vision, risk appetite, and overall strategic direction
- Approves plans to use the Assessment
- Reviews management’s analysis of the assessment results, as well as reviews or opinions on the results issued by independent risk management or the internal audit function
- Reviews management’s determination of whether the institution’s cybersecurity preparedness is aligned with its risks
- Reviews and approves plans to address any risk management or control weaknesses
- Reviews the results of management’s ongoing monitoring of the institution’s exposure to and preparedness for cyber threats

#### The CEO, with support from management
- Develops a plan to conduct the assessment
- Leads efforts to facilitate timely responses from across the institution
- Sets a target state of cybersecurity preparedness that is aligned to the board of directors’ risk appetite statement
- Reviews, approves and supports plans to address risk management and control weaknesses
- Analyzes and presents results to the executive team, key stakeholders and the board (or an appropriate board committee)
- Oversees the performance of ongoing monitoring to remain nimble and agile in addressing evolving areas of cybersecurity risk
- Oversees changes to maintain or increase the desired cybersecurity preparedness

---


9 Protiviti research has found a correlation between cybersecurity maturity levels and board engagement in information security management. Companies with engaged boards, and those with core information security policies in place, rate higher in their cybersecurity maturity: [www.protiviti.com/en-US/Pages/IT-Security-and-Privacy-Survey.aspx](http://www.protiviti.com/en-US/Pages/IT-Security-and-Privacy-Survey.aspx).
BENEFITS OF THE ASSESSMENT TO THE INSTITUTION

The Assessment is intended to help financial institutions and FFIEC member agencies make risk-informed decisions to identify and prioritize actions that enhance the effectiveness of cybersecurity programs and align them with the institution’s risk tolerance. As the third line of defense, internal audit, and IT audit in particular, should use the tool to ensure that the institution is effective in managing risk and is identifying instances where the institution has exceeded risk tolerance thresholds. Resulting actions may include business decisions that reduce inherent risk or investment to increase maturity in deficient cybersecurity processes and controls.

The Assessment complements institutions’ existing cybersecurity capabilities and risk management processes, and provides an additional input for institutions with key initiatives to improve the maturity of their cybersecurity capabilities. The concepts, processes and steps associated with completing the assessment should be familiar to internal audit professionals already versed in the principles contained in the FFIEC’s Information Technology (IT) Examination Handbook, along with other related industry standards, most notably the NIST framework.

UNDERSTANDING THE TOOL

The assessment tool expands on the FFIEC IT examination handbook by providing two main data points for institutions to consider and take action on: 1) The inherent risk profile of the institution and, 2) the institution’s overall cybersecurity maturity.

**Inherent risk**, according to the FFIEC, “incorporates the type, volume and complexity of the institution’s operations and threats directed at the institution. Inherent risk does not include mitigating controls.”

The inherent risk profile helps determine the level of risk exposure of the institution by collecting information related to the following areas:

- Technologies and connection types
- Delivery channels
- Online/mobile products and technology services
- Organizational characteristics
- External threats

Inherent risks are grouped into five categories – Least, Minimal, Moderate, Significant and Most – to help management identify and manage the company’s cybersecurity risk profile.

The cybersecurity maturity assessment provides institutions with the ability to determine their maturity in five cybersecurity domains:

- Cyber risk management and oversight
- Threat intelligence and collaboration
- Cybersecurity controls
- External dependency management
- Cyber incident management and resilience

Each of the domains is assigned a maturity rating of Baseline, Evolving, Intermediate, Advanced or Innovative. Determining the inherent risk profile of the institution is a responsibility of management. Internal audit is responsible for performing an independent validation of management’s assessment process. In performing the validation, internal audit should keep in mind that some areas within the maturity domains described above will pose greater risks than others, depending on the size and complexity of the institution and the products and services it provides.
ROLES AND RESPONSIBILITIES OF THE INTERNAL AUDIT FUNCTION

With the release of the Assessment, the internal audit function should be prepared to demonstrate to regulatory agencies that it has provided audit coverage of cybersecurity using the tool. If the institution is using an alternate cybersecurity assessment framework, such as ISO, COBIT, CSC or a proprietary framework, internal audit should be able to demonstrate how that framework’s approach and scope aligns with that of the FFIEC Assessment. Roles and responsibilities of internal audit include:

• Validating management’s assessment of cybersecurity maturity, associated findings, and sufficiency of plans to address weaknesses to align inherent risk and maturity
• Reporting to the board, or an appropriate board committee, the results of internal audit’s validation of management’s assessment
• Evaluating internal audit’s own level of maturity related to the cybersecurity audit process and strategy to determine if improvements are required to increase the effectiveness of internal audit as a third line of defense
• Contributing to the institution’s ability to manage cyber risk, in the capacity of an independent third line of defense, by performing regular audits of the institution’s cybersecurity processes and high-risk third-party vendors
• Continuously monitoring management’s progress in remediating cybersecurity control issues, reporting on remediation progress as needed, and performing independent validation of the remediation prior to closing the issue
• Planning for future cybersecurity audits to determine if management has integrated the FFIEC Assessment into enterprise risk management activities and reevaluating the institution’s inherent risk profile and cybersecurity maturity each time changes are planned that can potentially impact the risk/maturity alignment (e.g., launching new products or services, new connections, new delivery channels)
• If the institution has adopted an alternate cyber risk management framework, determining if management has taken steps to map the framework’s principles to the FFIEC Assessment and reporting on any gaps in coverage. Even more important, internal audit should determine if the alternate framework provides the means to manage risk, not just rate it – in other words, is management able to evaluate the institution’s current state of cybersecurity maturity against the institution’s inherent risk using the alternate framework?
• If management has not performed any, or recent, cybersecurity assessment activities within the first- or second-line functions, determining an appropriate approach for coverage and communicating directly to the board both the state of cybersecurity preparedness and the recommended approach based on the institution’s unique factors (e.g., known issues, most recent audit coverage)

Evaluating the Inherent Risk Profile

When evaluating the institution’s inherent risk profile, internal audit should include the following activities and considerations:

• Identify those individuals who contributed to the assessment and evaluate the appropriateness of their participation in the assessment.
• Verify that all necessary personnel were engaged in answering questions to determine the inherent risk profile regarding each category.
• Determine the sufficiency of documentation collected to support the determination of the institution’s inherent risk level.

---

10 Risk/maturity alignment is determined using the Risk/Maturity table included in the FFIEC Assessment.
• Verify that the inherent risk profile was focused on the appropriate legal entities of the institution over which the board, committees of the board, or the regulators have oversight. The risk profile should have considered all business units under the assessed legal entity, their products and services, and the technologies that enable them.

• Apply professional skepticism when determining if the inherent risk profile attributes were properly scoped for the organization.

It is important to note that internal audit may have a different view of the institution’s inherent risk or maturity assessment. If and when these differences are identified, internal audit should be prepared to provide information that supports their view and work with management to agree on a common view of inherent risk. If a common view cannot be achieved and internal audit is firm in their opinion (based on factual findings), the issue should be raised to the board or an appropriate board committee.

Evaluating the Cybersecurity Maturity Assessment

To evaluate the cybersecurity maturity assessment completed by management, internal audit needs to do the following:

• Understand what activities management has performed to determine the maturity ratings for each cybersecurity domain, and determine whether each declarative statement used to support the rating is sufficiently backed by evidence of an appropriate activity.

• Determine if all declarative statements for each domain’s maturity level, as well as the levels below it, have been attained or else determined to be irrelevant to the institution.

• Independently verify a sample of declarative statements within the maturity level determined by management by inspecting the relevant documentation or observing the activities performed.

• Identify all declarative statements determined as not applicable to the institution by management and independently review management’s rationale as to the appropriateness and accuracy of the determination.

• Verify that management’s maturity ratings are consistent with the aggregation of open issues identified by internal audit as well as sources outside of internal audit, including the institution’s regulators, management itself, and any independent third parties performing assessments on behalf of management.

• Identify and follow up on any discrepancies between management’s and internal audit’s views of the cybersecurity maturity rating.
Evaluating Management’s Interpretation and Analysis of the Assessment Results

If management has determined that the institution’s cybersecurity maturity levels are not on par with its inherent risk profile, based on the risk/maturity relationship table included in the Assessment, internal audit needs to know what steps are being taken to reduce inherent risk or improve cybersecurity maturity levels. For example, internal audit needs to determine whether management has conducted a gap analysis, set target maturity levels appropriate to the inherent risk profile, planned and prioritized actions to bring inherent risk and cybersecurity maturity into alignment, implemented changes, reevaluated changes made over time, and communicated the results to executive management, the board or an appropriate committee of the board. Additional actions to be taken by internal audit in evaluating management’s interpretation and analysis of assessment results include the following:

- Determine if the institution’s risk management function has a view of the institution’s inherent risk profile that differs from that of management. If so, understand what factors are contributing to the difference.
- Determine if the institution has formally developed risk tolerance thresholds. If so, determine if the organization’s risk tolerance thresholds differ from or agree with those identified in the Assessment’s risk/maturity relationship table.
- Inquire with management and appropriate personnel to determine whether remedial actions (actions directed at reducing the institution’s risk profile or improving its cybersecurity maturity) have been formally associated with projects, and that the projects have been funded by the institution.
- Perform ongoing monitoring of the projects associated with remedial actions.

CONCLUSION

For most institutions, cybersecurity is a top risk, and a cybersecurity event is only a matter of time. Financial institutions must not delay their adoption of the cybersecurity assessment tool the FFIEC has developed if they are to have a chance in this race against time. The tool can help internal audit functions identify with precision the specific factors that drive the institution’s overall cybersecurity risk, determine the specific activities associated with effective cybersecurity, evaluate the institution’s preparedness for a cyberattack, and recommend specific risk management practices and controls that can be implemented to strengthen preparedness. The clock is ticking; getting started with the Assessment now is the best way for institutions and their internal audit functions to address this top risk.
ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 Fortune 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How We Help Companies Succeed

We work with audit executives, audit committees and management at companies of any size, public or private, to assist them with their internal audit activities – from strategic advice around the structure and objectives of the IA function, to developing and implementing tools and processes, augmenting audit teams with subject-matter expertise and providing highly-trained resources to assist with audit execution.

Our specialized team of IT audit professionals partners with internal audit departments at financial organizations to help them gain insight into the threats inherent in today’s highly complex technologies and identify and evaluate appropriate control activities to ensure the integrity, reliability and security of their IT systems.

Our IT audit services include:
- Cybersecurity assessments
- Vendor risk assessments and due diligence reviews
- Vulnerability assessments
- ISO/SOC certification readiness assessments
- IT risk assessments
- Application security assessments
- Technology infrastructure assessments

Contacts

<table>
<thead>
<tr>
<th>Jim Armetta</th>
<th>Matthew Mueller</th>
<th>Michael Thor</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1.212.399.8606</td>
<td>+1.212.708.6310</td>
<td>+1.317.510.4685</td>
</tr>
<tr>
<td><a href="mailto:james.armetta@protiviti.com">james.armetta@protiviti.com</a></td>
<td><a href="mailto:matthew.mueller@protiviti.com">matthew.mueller@protiviti.com</a></td>
<td><a href="mailto:michael.thor@protiviti.com">michael.thor@protiviti.com</a></td>
</tr>
</tbody>
</table>
THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston

ARGENTINA*
Buenos Aires

BRAZIL*
Rio de Janeiro
São Paulo

CANADA
Kitchener-Waterloo
Toronto

EUROPE/MIDDLE EAST/AFRICA

FRANCE
Paris

GERMANY
Frankfurt

ITALY
Milan

THE NETHERLANDS
Amsterdam

UNITED KINGDOM
London

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

SOUTH AFRICA*
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*Protiviti Member Firm