Table of Contents

A. Editorial Note from the Managing Director, Center of Regulatory Intelligence ................................................................. 3
B. Semimonthly Washington, D.C. Regulatory Round Up ........................................................................................................ 5
C. Featured Regulatory Intelligence Briefing: FFIEC Cybersecurity Assessment ................................................................. 9
D. Did You Know? ........................................................................................................................................................................ 19
E. About FIS’ Center of Regulatory Intelligence ................................................................................................................. 21
A. Editorial Note from the Managing Director, FIS Center of Regulatory Intelligence

Introduction

Welcome to the first edition of FIS’ semimonthly Regulatory Intelligence Briefing (RIB). FIS clients will have the opportunity to receive insights from the Center through the RIB, which will contain articles and thought-leadership intended to give institutions deep intelligence into regulatory initiatives coming out of the legislature, administration and regulatory agencies. This inaugural edition provides our valued clients with guidance on how to effectively incorporate the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (Cybersecurity Assessment) and the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity into their risk management framework.

The FFIEC Cybersecurity Assessment Tool dramatically changes how financial institutions address cybersecurity by establishing a prescriptive method to assess cybersecurity preparedness on an ongoing basis. Examiners will start using the tool, and the regulatory expectation is that each institution will complete the Cybersecurity Assessment and maintain it. This RIB dissects the Cybersecurity Assessment and provides actionable intelligence to help you navigate the next steps, know what is expected under the assessment and, perhaps most importantly, advise you on what to do next. While we focus on the new FFIEC Cybersecurity Assessment Tool in this edition, FIS will continuously monitor and analyze the FFIEC’s workstream to coordinate across federal and state regulatory agencies. We will keep you informed and prepared to respond to the seven key areas on which the FFIEC is focused, including:

1. Cybersecurity Self-Assessment Tool
   The FFIEC plans to issue a self-assessment tool this year to assist institutions in evaluating their inherent cybersecurity risk and their risk management capabilities.

2. Crisis Management
   The FFIEC will align, update, and test emergency protocols to respond to system-wide cyber incidents in coordination with public-private partnerships.

3. Policy Development
   The 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, cybersecurity controls, external dependency management, and incident management and resilience.

4. Collaboration with Law Enforcement & Intelligence Agencies
   The FFIEC will build upon existing relationships with law enforcement and intelligence agencies to share information on the growing cybersecurity threats and response techniques.

5. Incident Analysis
   FFIEC members will enhance their processes for gathering, analyzing, and sharing information with each other during cyber incidents.

6. Training
   The FFIEC will develop training programs for the staff of its members on evolving cyber threats and vulnerabilities.

7. Technology Service Provider Strategy
   The FFIEC’s members will expand their focus on technology service providers’ ability to respond to growing cyber threats and vulnerabilities.
While large and small organizations alike must perform risk assessments to comply with numerous regulatory requirements, the FFIEC and NIST have looked to provide a series of best practices and tools without adding to the burden of a growing list of compliance challenges. With that in mind, the challenge for institutions is when trying to understand regulator expectations and the point at which examiners shift from “voluntary” to “expected” to “required” during an examination.

The Cybersecurity Assessment published by the FFIEC comes on the heels of the U.S. government’s response to hackers’ and nation-states’ exploitations of computer networks across the globe. These include large-scale and high-profile attacks on retailers and, most recently, the U.S. Office of Personnel Management (OPM), which media reports indicate impacted an estimated 21 million people. U.S. policymakers continue to strive to address the growing dangers of cybersecurity and hacker attempts to access and undermine our government, national defense and economic interests, especially in the banking and financial services sectors.

The U.S. Congress plays a pivotal role in protecting critical infrastructure and information systems – federal and nonfederal alike – from cyberattacks, as well creating appropriate regulatory structures to address potential emerging threats to the financial stability of the U.S. To that end, the U.S. House of Representatives has passed legislation that allows for a mechanism to enable sharing of cybersecurity information between private and government entities. Additional enacted legislation mandates notice to individuals affected by a security breach. These are positive steps toward addressing cybersecurity concerns facing American consumers.

I attended several congressional hearings on cybersecurity over the last several months, including a May 14, 2015 House Financial Services Committee hearing entitled “Protecting Consumers: Financial Data Security in the Age of Computer Hackers.” At this hearing, Chairman Jeb Hensarling (R-TX) spoke about the increased risks to consumers with regard to theft of their personal financial information and highlighted how current cyberattack methods make this a profitable enterprise for cyber criminals and computer hackers. In the U.S. Senate, U.S. Senate Majority Leader Mitch McConnell (R-KY) has called for a vote in July on S.754, “Cybersecurity Information Sharing Act of 2015” (CISA), to improve cybersecurity information sharing between the government and the private sector, including liability protections for companies that share information on threats or breaches after a cyberattack. We will continue to closely monitor these legislative initiatives.

In our next RIB, we will explore the key areas on which banks, credit unions and others in the industry must focus to ensure compliance with the much anticipated October 3 deadline for the Consumer Financial Protection Bureau’s (CFPB) Integrated Mortgage Disclosures Rule under the Real Estate Settlement Procedures Act (Regulation X) and the Truth in Lending Act (Regulation Z). We look forward to continuing to be your partner in risk, information security and compliance, and delivering timely actionable intelligence to you so you can make smart business decisions and stay proactive.

**Peter D. Dugas**  
*Managing Director, FIS Center of Regulatory Intelligence*

Peter has over 16 years of government and consulting experience in advising clients on supervisory matters before the U.S. Government and in the implementation of enterprise risk management programs. He is a thought-leader in government affairs and regulatory strategies in support of banks and financial institutions compliance with the Dodd-Frank Act and Basel Accords. Prior to joining FIS, he served as a Director of Government Relations at Clark Hill PLC and in senior government positions, including serving as a Deputy Assistant Secretary at the U.S. Department of the Treasury.
B. Semimonthly Washington, D.C. Regulatory Round Up

Regulatory and Compliance Alerts

FDIC Issues Financial Institution Letter (FIL) on Federal Financial Institutions Examination Council (FFIEC) developed Cybersecurity Assessment Tool

On July 2, 2015, the FDIC issued a Financial Institution Letter (FIL) for all FDIC-supervised institutions, which encourages institutions to comment on the usability of the Cybersecurity Assessment Tool and informs supervised institutions that examiners will discuss the Cybersecurity Assessment Tool with institution management during examinations to ensure awareness and assist with answers to any questions.

SEC Proposes Rules Requiring Companies to Adopt Clawback Policies on Executive Compensation

On July 1, 2105, the U.S. Securities and Exchange Commission (SEC) proposed rules for national securities exchanges and associations to adopt policies requiring executive officers to “clawback” incentive-based compensation due to an accounting restatement.

The policies are intended to impact current and former executive officers’ compensation that are tied to accounting-related metrics, stock price, or total shareholder return. Executive officers affected by the policies could see recovery from excess incentive-based compensation received in the three fiscal years preceding the date a listed company is required to prepare an accounting restatement.

Supreme Court Ruling on Disparate Impact

On June 25, 2015, the Supreme Court of the United States published a decision in the case of Texas Department of Housing and Community Affairs et al. vs. Inclusive Communities Project, Inc. The significant issue is whether a claim of disparate impact discrimination can be made under the Fair Housing Act. Disparate impact claims are based on the discriminatory effect of a particular practice, rather than evidence of a discriminatory intent.

In this case, a Texas housing agency practice of awarding federal tax credits to construct affordable housing more often in predominantly black urban areas of Dallas than in predominantly white suburban neighborhoods was challenged by a community housing organization. The claim of the organization is that the housing agency practice has a disparate impact and violates the Fair Housing Act because favoring the construction of affordable housing in minority neighborhoods perpetuates segregated housing patterns.

The position set forth by Texas is that the Fair Housing Act does not provide authority for the theory of disparate impact liability.

The Supreme Court concluded that disparate impact claims (with some limits) are cognizable under the Fair Housing Act.

CFPB Delays Integrated Mortgage Disclosure Implementation Date

In a June 24, 2015, press release, CFPB Director Richard Cordray announced that the current August 1, 2015 implementation date for the new integrated mortgage disclosures will be delayed until October 3, 2015.

The Bureau has proposed a rule to extend the effective date. As with other proposed regulatory amendments, it was open for public comment before a final rule is published.
Agencies Issue Flood Insurance Final Rule

In a June 22, 2015 joint press release, the federal regulatory agencies (Federal Reserve Board, Farm Credit Administration, Federal Deposit Insurance Corporation, National Credit Union Administration and Office of the Comptroller of the Currency) announced a joint final rule to amend regulations that apply to loans secured by properties located in special flood hazard areas. The final rule implements provisions of the Homeowner Flood Insurance Affordability Act of 2014 (HFIAA) relating to the escrowing of flood insurance payments and the exemption of certain detached structures from the mandatory flood insurance purchase requirement. The final rule also implements provisions in the Biggert-Waters Flood Insurance Reform Act of 2012 relating to the force placement of flood insurance.

NCUA Proposes Changes to Member Business Loan Regulation

In a June 18, 2015 press release, the National Credit Union Administration (NCUA) announced a proposed rule to provide federally-insured credit unions greater flexibility and autonomy to offer member business loans.

As proposed, the rule will give credit union loan officers the ability to waive a personal guarantee; remove explicit loan-to-value limits and eliminate the need for a waiver process; lift limits on construction and development loans; and clarify that non-member loan participations will not count against the statutory member business lending cap.

Treasury Publishes Risk Assessments on Money Laundering and Terrorist Financing

On June 12, 2015, the Department of the Treasury published the National Money Laundering Risk Assessment (NMLRA) and the National Terrorist Financing Risk Assessment (NTFRA). The purpose of these assessments is to help the public and private sectors understand the money laundering and terrorist financing methods used in the United States; the risks that these activities pose to the U.S. financial system and national security; and the status of current efforts to combat these methods. These assessments may assist the federal government and financial institutions in detecting and combatting illicit finance. This type of analysis was last published in 2005.

The NTFRA report finds that the United States has made it substantially more difficult for terrorist organizations to raise and move money through the U.S. financial system since the September 11, 2001 attacks. A notable trend is a decrease in the use of the U.S banking system for terrorist financing-related transactions.

CFPB to Oversee Nonbank Auto Finance Companies

In a June 10, 2015 press release, the CFPB announced a final rule concerning the supervision of larger nonbank auto finance companies. The Bureau also released the procedures that will be used to examine auto finance companies.

Any nonbank auto finance company that makes or acquires 10,000 or more loans or leases in a year is considered a "larger participant" and will be subject to CFPB supervision. The Bureau estimates that 34 lenders will be monitored for compliance with federal consumer protection requirements.

The final rule will be effective 60 days after publication in the Federal Register.
Legislative Activity

U.S. House of Representatives

Majority Leader Kevin McCarthy (R-CA) released a memorandum outlining the remaining legislative priorities for the month of July. Of particular interest, the House is expected to vote on H.R. ____ the “Fiscal Year 2016 Financial Services and General Government Appropriations Act,” authorizing $20.2 billion in funding for FY 2016, which is $1.3 billion below FY 2015 enacted levels and $4.8 billion below President Obama’s FY 2016 budget request. The bill will fund the U.S. Department of the Treasury, CFPB, the Small Business Administration (SBA), the SEC and other federal departments and agencies.

The House will also consider H.R. 427, the “Regulations From the Executive in Need of Scrutiny Act” (“REINS Act”), requiring the Congress to approve all new major regulations and allow the courts to review whether an agency in the rulemaking process completed the necessary requirements for the proposed rule to take effect. Both bills are anticipated to pass the House due to a Republican majority, but the bills’ fate in the U.S. Senate will have a steeper challenge.

Legislation

H.R.2596: “Intelligence Authorization Act for Fiscal Year 2016” A bill sponsored by Rep. Devin Nunes (R-CA-22) to authorize FY2016 appropriations for the conduct of intelligence and intelligence-related activities for certain federal departments and agencies. The bill establishes a Cyber Threat Intelligence Integration Center (CTIIC) within the Office of the DNI to serve as the primary organization within the federal government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to cyberthreats, and share and coordinate cyberthreat intelligence activities and strategic planning with appropriate federal agencies. Passed 247 – 178. Statement of Administration Policy.


H.R.1770: “Data Security and Breach Notification Act of 2015” A bill sponsored by Rep. Marsha Blackburn (R-TN) to require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving the information. Passed House Energy and Commerce Committee 29 – 20.

H.R. 1195: “Bureau of Consumer Financial Protection Advisory Boards Act” A bill sponsored by Rep. Robert Pittenger (R-NC) to direct the Director of the CFPB to establish a Small Business Advisory Board. Under the rule for consideration, a provision was included to limit funding for the CFPB to $655 million for FY 2020 and $720 million for FY 2025. Passed 235 – 183. Statement of Administration Policy.
**H.R. 234:** A bill sponsored by Rep. Dutch Ruppersberger (D-MD) to provide for the sharing of cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes. Referred to the Subcommittee on the Constitution and Civil Justice.

**U.S. Senate**


**Legislation**

**S.1376:** “National Defense Authorization Act for Fiscal Year 2016” A bill sponsored by Sen. John McCain (R-AZ) to authorize FY2016 appropriations and policies regarding the military activities of the Department of Defense (DOD), military construction and the defense activities of the Department of Energy (DOE). The bill contains provisions to provide for acquisition of cyberoperations and training, identification and mitigation of cybervulnerabilities of major weapon systems, assessment of offensive and defensive cybercapabilities of China and Iran, and authorization of military cyberoperations. Placed on Senate Legislative Calendar.

**S. 961:** “Data Security Act of 2015” A bill sponsored by Sen. Thomas Carper (D-DE) to establish strong and uniform national data security and breach notification standards and to expressly preempt any related State laws in order to provide the Federal Trade Commission with required information. Referred to the Committee on Commerce, Science, and Transportation.

**S. 754:** “Cybersecurity Information Sharing Act of 2015 (CISA)” A bill sponsored by Sen. Richard Burr (R-NC) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. Passed Senate Select Committee on Intelligence (SSCI) on a vote of 14 to 1.

**S. 456:** “Cyber Threat Sharing Act of 2015” A bill sponsored by Sen. Thomas Carper (D-DE) to permit private entities to disclose lawfully obtained cyberthreat indicators to a private information sharing and analysis organization and receive indicators disclosed by parties. Referred to the Committee on Homeland Security and Governmental Affairs.
C. Featured Regulatory Intelligence Briefing: FFIEC Cybersecurity Assessment

Cybersecurity Threat Trends

The latest headlines on the theft of personal information, credit cards and healthcare records continue unabated – in and out of the industry – about whether financial institutions are doing enough to protect consumers’ critical information and their assets. Just a few months ago, the U.S. Office of Personnel Management (OPM) reported that over 21 million government personnel files were illegally accessed, reportedly by Chinese cyberattackers. Fewer than ten days prior to the OPM breach, the Internal Revenue Service (IRS) reported that the personal information of nearly 100,000 taxpayers was obtained by a Russian cybercriminal syndicate.

Lastly, in the biggest cybersecurity breach of the year, the health records of more than 80 million Anthem Healthcare customers were stolen by cybercriminals. As these incidents illustrate, the sheer number and scale of cybersecurity breaches is accelerating at an alarming rate. One would think that by now, a methodical and effective strategy for defending information against these threats must exist. Unfortunately, it’s been a mixed bag of regulatory guidance – until now.

On June 30, 2015, the FFIEC, which represents a consortium of Bank examiners (including the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the CFPB), published a Cybersecurity Assessment Tool, which is profiled in depth within this brief. Among the various assessment methods available today, it is the most specific guidance available on performing a cybersecurity risk assessment at a financial institution.

While any organization could perform a full-court press of the assessment from start to finish, it is clear from the assessment itself that the FFIEC is implying an order of importance amongst the various aspects of the assessment. It is our assertion that knowing the order of importance is critical for any organization to quickly, efficiently and successfully complete the assessment to effectively protect the enterprise and stay ahead of the risks.

The Need for a Risk-Based Approach to Cybersecurity

Before we dive into the new assessment, let’s look briefly at how we got here. In response to increasing cybersecurity risk, government agencies, private companies and non-profit organizations alike needed to react quickly. Due to the shared risk presented by cybersecurity challenges, public and private-sector entities collaborated to publish guidance on cybersecurity assessments.
The NIST Cybersecurity Framework is an early example of these initiatives; however, it suffered from being too high level. It answered the question:

“What is everything we need to do to address cybersecurity risks?” without answering the questions, “Where are we now?” and “Where do we need to be?”

As a result, the FFIEC started a working group to study the specific impact of cybersecurity issues for financial institutions. This work culminated in the Cybersecurity examination pilot program pilot during the summer of 2014, with the goal of evaluating the state of cybersecurity preparedness and mitigating cyberattacks across 500 financial institutions. The review focused on two factors. First was the concept of Inherent Risk. This is risk presented by the number and complexity of connection types, products and services offered, and technologies used. This is the starting point that answers the question, “How risky are my operations?” Part 2 of the review involved concepts related to Cybersecurity Preparedness, or the degree of sophistication an institution has with regard to management oversight, threat intelligence, cybersecurity controls, vendor management and incidents.

While the pilot program hinted at the need for a risk-based approach to cybersecurity that recognizes an organization’s unique set of risks; it generated more questions than answers for the participating institutions. For example, “What are the attributes of high inherent risk versus low inherent risk?” “How does inherent risk influence the level of sophistication of my controls?” And ultimately, “Am I on track if a cybersecurity examination occurs today?”

FFIEC Cybersecurity Assessment Tool

To address these concerns, the FFIEC, on behalf of its members, released the aforementioned Cybersecurity Assessment Tool to provide very specific guidance to C-level management, Boards of Directors and other users of the tool. Drawing upon some of the research already conducted by the Institute of Internal Auditors and Information Systems Audit Control Association, the FFIEC makes clear that CEOs and Boards of Directors have the responsibility to:

Plan the assessment
Lead and facilitate timely responses across the institution
Set target dates
Review, approve, and support a plan to address weaknesses
Analyze and present results
Remain agile in areas of emerging cybersecurity risk
Oversee changes that are necessary to increase cybersecurity preparedness

This is not something senior leadership can simply delegate away. In other words: Cybersecurity is a boardroom business issue, not a back-office technology problem.
As a boardroom business issue, the Cybersecurity Assessment requires executives to take a methodical approach to assessing the organization’s inherent risk in business terms. Just like the pilot program, it asks specific questions about:

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

Unlike the pilot program, however, the Cybersecurity Assessment dives further into specifics that provide the following inherent risk ratings:

- Least
- Minimal
- Moderate
- Significant
- Most

These inherent risk ratings are critical to maintaining awareness of where an organization stands today. It’s the anchor point of how cybersecurity maturity levels relate to institutional risks. The underlying concept here is that the higher the level of inherent risk, the greater the demand is with regard to the sophistication of cybersecurity capability. The tool refers to this as “Maturity.”

Maturity is an estimate of the sophistication (or lack thereof) an organization may have in defending against a cyberattack. Maturity is described among five domains:

- Domain 1: Cyber Risk Management and Oversight
- Domain 2: Threat Intelligence and Collaboration
- Domain 3: Cybersecurity Controls
- Domain 4: External Dependency Management
- Domain 5: Cyberincident Management and Resilience

Each domain is rated at a maturity between:

- Baseline
- Evolving
- Intermediate
- Advanced
- Innovative
Stay In the Blue Square!

To understand how all of this comes together, take a look at following matrix developed by the FFIEC:

Without going into the details of every domain, you should understand that, if an institution aligns itself with the recommendations published in the FFIEC Examination Handbook, the organization will be automatically considered “Baseline” maturity within each domain. The rub here is, should there be greater institutional complexity from an inherent risk rating perspective, the examiner’s expectations for maturity will increase.

For example, say that an institution’s inherent risk rating is Moderate, but only complies with the baseline level of maturity. Based on the matrix above, the institution will fall on a white square. Anything falling on a white square is a warning. In our example, it should be a warning to management to take a closer look at what it would take to reach an Evolving level of maturity, which is indicated by a blue square. A blue square represents the FFIEC’s expected level of maturity.

This does not mean that simply looking at the requirements for Evolving Maturity and meeting them will move the institution into the blue square. The effects are cumulative, not exclusive. In this scenario, the institution must maintain the Baseline Maturity designation and the requirements of the Evolving Maturity designation.
**Actionable Intelligence – Key Triggers to Watch**

Financial institutions that currently oversee risk management through a risk committee should consider key triggers to watch for that may impact their inherent risk rating.

![For example:]

Is there a trend to move critical operations from a private network to the public cloud?  
Is the institution moving away from a retail branch strategy to an Internet only Bank?  
Are payments increasingly reliant on mobile and online channels and third parties?  
Is the organization changing from in-house to outsourced contract staff and contractors, especially for security services?  
Is the security monitoring system indicating increased number of threats from the outside?  
What is the impact of a new product or service to the overall risk profile?  
Does the institution plan to merge or acquire another organization? Why kinds of cybersecurity risks will be introduced? Is it possible to assume the risk?

All of these triggers represent opportunities to revisit the inherent risk ratings and conduct an additional assessment. As change is constant in most organizations, financial institutions should use the Cybersecurity Assessment Tool on a continuous and ongoing basis. It should be not used as a “check the box” or single point-in-time activity.

**Not All Domains Are Created Equal**

Now that we have a grasp on the mechanics of the Cybersecurity Assessment Tool, let’s turn our attention to the domains themselves. While meant to be comprehensive in its approach, there is a lot of ground to cover. The reality is that most organizations have limited time, budget and resources to conduct an assessment from start to finish. Critical questions present themselves such as:
The good news here is that not all domains are created equal. By observing the past, present and anticipated future FFIEC guidance, along with the sheer volume of content, one can clearly read the tea leaves. The following section describes FIS’ recommendation for how financial institutions should align their priorities and why.

Considering the fact that the FFIEC published two specific statements on March 30, 2015 on compromised credentials and destructive malware, this tips their hat as to what they think is really important in the Cybersecurity Assessment Tool. Recognizing that compromised credentials (especially privileged accounts) and destructive malware are particularly disruptive to a bank’s operations, it is clear that:

- **Domain 3: Cybersecurity Controls**, under the assessment factor of Preventive and Detective controls, is incredibly important. *Key themes to pay close attention to are Device/End Point Security and Anomaly Activity Detection.* It is also worth noting that the largest part of the assessment is comprised of Domain 3.

- **Domain 2: Threat Intelligence and Collaboration.** This is a short but a big part of the FFIEC Cybersecurity Strategy. Why? A couple of factors support this conclusion. It is no secret that government agencies don’t effectively share threat information among themselves or with private industry. Critical threat information may be missed simply because organizations do not work well with each other. Therefore, there is an enormous need for government agencies and security organizations to share threat information with private industry to be ahead of emerging and new threats.

The Cybersecurity Information Sharing Act of 2015 is emblematic of this. Although it has yet to pass Congress, it is on the right conceptual track. Unfortunately, cyber attackers do not have to go through the same drawn out government or policymaking processes to share information or to plan their next attack. Critical to the success of cyberattacks is their ability to collaborate instinctively, naturally, freely and securely, much to the dismay of government agencies and private companies.
Additionally, the FFIEC has a targeted working group set up to investigate robust information sharing among law enforcement and intelligence agencies. As it relates to the Cybersecurity Assessment Tool, be sure to take a long, hard look at the threat data you are consuming, and make sure you can convert it into actionable intelligence.

The remaining domains fall into place simply by following the planned FFIEC workgroup deliverables. Incident analysis has a logical next step because it builds upon information sharing capabilities in Domain 2, except it targets the process of sharing cybersecurity incident information. Along with crisis management and understanding protocols to respond to system-wide cyber incidents that involve public and private companies:

- **Domain 5: Cyber Incident Management and Resilience** should be considered the third important aspect of the Cybersecurity Assessment Tool.

Once you have addressed the top three, the remaining two domains will sound different under the tool, but in most cases will be part of the risk management process already in place. Leveraging **Domain 4: External Dependency Management**, the Cybersecurity Assessment Tool can augment your institution’s existing vendor assessment techniques to evaluate whether critical vendors are considering cybersecurity risks as part of their reports to the Risk Committee.

- **Domain 1: Cyber Risk Management & Oversight**, lastly, is the domain for which most organizations will have various internal management committees that ultimately report to the Board. This domain highlights cybersecurity aspects related to the “tone at the top” with regard to cybersecurity topics, as well as the control and management structures necessary to effectively implement a cybersecurity risk management program. These committee structures can be effectively evaluated and enhanced using the tool.

**Community, Regional Bank and Credit Union Pitfalls**

While the priorities asserted above apply to all institutions, special consideration should be given to community and regional banks and credit unions when it comes to the FFIEC Cybersecurity Assessment Tool. Typically, these institutions and credit unions may need to adjust their priorities based on the fact the some or all of the IT services and operations are outsourced to a vendor. When outsourcing critical IT services and business operations to a vendor, under the provisions of the Cybersecurity Assessment tool, the level of maturity expected is higher than the Baseline designation, even though the institution and credit union may not directly control the service provider.

In fact, the top three domains under these circumstances might be under the exclusive control of the service provider. It is, therefore, critical that institutions and credit unions under these conditions prioritize **Domain 4: External Dependency Management** as their top priority.

The GAO Report on Cybersecurity further supports this priority as it hints of a future where the FDIC, the primary regulator for a large number of small banks, might be given the right to examine third party service providers as part of a comprehensive cybersecurity review of a small bank. Finally, the GAO report points to a future in which small bank examiners will be more technically savvy and able to assess risks not just from an individual institution perspective, but rather across many institutions sharing similar third-party service providers and, more importantly, cyberthreat and incident data.
What this means for smaller institutions is that the examiner may not only ask, “Are you monitoring for cybersecurity threats?”, but rather, “How do you correlate the information to make it actionable?” To answer that question, an institution may have to take a serious look at how your IT service provider is aligned with the FFIEC Cybersecurity Assessment Tool, at least among the first three domains.

**Regulatory Expectations**

The bottom line is that each financial institution is expected to use the Cybersecurity Assessment. First, it should be used to identify an inherent risk level:

![Risk/Maturity Relationship vs. Inherent Risk Levels Chart](chart1)

Next, the Cybersecurity Assessment should be used to identify the maturity level for each of the five domains:

![Cybersecurity Assessment Domains](chart2)

(United States. Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool” Overview for Chief Executive Officers and Boards of Directors”, pp. 3-4, June 2015)
Finally, institutions are expected to use the Cybersecurity Assessment to identify gaps and a target maturity state for each of the five domains, as well as an action plan to attain and sustain the maturity level:

The FFIEC Cybersecurity Assessment will not only be used by examiners to assess a financial institution’s cybersecurity preparedness, but the regulatory expectation is that every single financial institution will use the Cybersecurity Assessment to identify cybersecurity inherent risk and maturity levels, implement an action plan to attain and sustain the target state, and periodically update the Cybersecurity Assessment. The Board of Directors and CEO are ultimately responsible for ensuring that the Cybersecurity Assessment is completed properly and timely and updated periodically.
Conclusion

The FFIEC Cybersecurity Assessment Tool will have a significant impact on financial institutions large and small. Examiners will start using the Cybersecurity Assessment in future exams. There is a clear regulatory expectation that every single institution should use the Cybersecurity Assessment and periodically make updates based on changes to their risk profiles. It is a comprehensive, risk-based approach that is tailored to the cybersecurity risks faced by financial institutions today. To stay ahead of cybersecurity risks as well as examiner scrutiny, there is an order of importance that is implied in the Assessment itself, which will help organizations prioritize what areas they should consider first using the finite resources available to quickly achieve desired outcomes.

If you’ve enjoyed this Regulatory Intelligence Bulletin and are interested in further dialogue, please contact one of FIS’ subject matter experts on the FFIEC Cybersecurity Assessment Tool and any other aspects of our risk, information security and compliance services.

Andrew C. Kim
Director, Technology Risk Management – Cybersecurity

Andy has over 15 years of Cybersecurity, Information Security, IT Audit, Security Operations, Business Continuity Planning and Disaster Recovery experience within the Banking, Investment Management, Insurance and Healthcare industries. Andy holds multiple information security certifications. Prior to joining FIS, Andy was the Chief Information Security Officer (CISO) at a large financial institution. Originally coming from a high availability mission critical Internet infrastructure background, Andy has implemented enterprise class cybersecurity and information security programs from large franchise banking organizations to small entrepreneurial pre-IPO companies. This unique set of experiences allows Andy to provide a tailored approach to technology risk management, balancing risk with strategic business objectives.
D. DID YOU KNOW?

CyberForce

FIS has launched CyberForce™, a state-of-the-art data analytics software that detects the most critical cybervulnerabilities for timely risk mitigation so a cyberdisaster can be prevented. The FFIEC Alert issued on March 31, 2015, and the Cybersecurity Assessment issued on June 30, 2015, establish regulator expectations for ongoing monitoring and timely detection of privileged user credential hijacking or compromise. CyberForce timely detects this cyber risk, among others, and enables a rapid response to prevent loss.

CyberForce Delivers Next-Gen Rapid Detection and Response

CyberForce On-Premise License

Cybersecurity Assessment

FIS cybersecurity experts are highly experienced and intimately familiar with the FFIEC Cybersecurity Assessment and can help you complete the Assessment properly and timely. We can also provide ongoing updates and maintenance. Our experts possess a vast knowledge base of cybersecurity best practices and deep expertise on the NIST cybersecurity framework, the foundation for the FFIEC Cybersecurity Assessment. You cannot afford to miss the mark. The stakes are very high.

Use FIS cybersecurity experts to complete your Assessment properly and timely before your next exam, avoid regulatory enforcement action and protect your reputation.

Our cybersecurity consultants are domain experts who formerly served in these roles:
- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- IT auditor
- Bank regulator
- Bank examiner
- Forensic examiner
- Law enforcement

Read More:
E. About FIS Center of Regulatory Intelligence

FIS™ (NYSE: FIS), a global leader in banking and payments technology as well as consulting and outsourcing solutions, opened its Center of Regulatory Intelligence (“Center”) in Washington, D.C. on June 16, 2015. The primary goal of the Center is to translate policy, legislative and regulatory developments into actionable intelligence for FIS clients to enable knowledge advantage. The unique perspective gained by monitoring regulatory change at such close proximity to the policy makers and regulators will enable the Center to empower FIS clients to stay one step ahead, identify impact precisely, make smart business decisions and succeed. FIS clients will have the opportunity to receive insights from the Center through regularly published regulatory intelligence briefings and thought leadership insights intended to give client institutions deep intelligence into regulatory initiatives coming out of the legislature, administration and regulatory agencies. Input from the center also will help drive FIS research and development efforts as well as consulting services aimed at helping institutions address regulatory changes prior to implementation.

The Center provides the latest intelligence, thought leadership and cutting-edge regulatory insights into risk, information security and compliance issues facing the financial services industry. This new FIS thought leadership Center will provide early insight on regulatory changes, helping financial services clients stay compliant with new regulations. Through the Center, FIS will interface with key policymakers to provide industry perspectives on the potential impacts of regulatory mandates to financial institutions.

Contact Us

FIS Center of Regulatory Intelligence
1101 Pennsylvania Ave., NW Suite 600
Washington, DC 20004
E: fis.cri@fisglobal.com
P: 202.756.2263