

RESILIENCE THROUGH NATURAL DISASTERS



CAPCO
THE FUTURE. **NOW.**



IN THIS ISSUE

**EDITORIAL NOTE FROM
THE MANAGING PRINCIPAL,
CENTER OF REGULATORY
INTELLIGENCE** 3

REGULATORY ROUNDUP 4

**FOCUS: RESILIENCE THROUGH
NATURAL DISASTERS** 5

INTRODUCTION 5

KNOW YOUR RISKS 6

DEVELOPING A BCP 7

BEING THERE FOR YOUR COMMUNITY 11

CONCLUSION 12

**CONGRESSIONAL HEARING
SUMMARY: FRB SEMIANNUAL
TESTIMONY** 13

CONTACT US 18

EDITORIAL NOTE FROM THE MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE



PETER D. DUGAS
MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE

Peter has more than 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 Capco, he served as a director of government relations at Clark Hill and in senior government positions, including serving as a deputy assistant secretary at the United States Department of the Treasury.

2018 has been a difficult year for many regions in the U.S. that suffered from natural disasters. By halfway through the year, the country had [already seen](#) six individual natural disasters with damages estimated over 1 billion for each. By October, the count was [up to 11](#), and including events within the past month, 2018 is set to be one of the most costly years of natural disasters in recent history; and studies show the trend is set to continue. For financial institutions, resiliency through natural disasters is becoming increasingly critical.

In the financial services industry, consumers and regulators require institutions to have sufficient plans to ensure minimal operational disruption following a natural disaster. Failure to appropriately prepare can not only put an institution at risk for operational failure, but also expose the institution to unfavorable regulatory action and reputational damage. Institutions must learn from the events of the past few years, and evolve their planning to properly align with their needs and risks, including operational and community considerations.

In this month's Regulatory Intelligence Briefing (RIB), Center for Regulatory Intelligence (CRI) considers all aspects of a financial institution's resilience through natural disasters. We review various areas often forgotten, the impact these oversights can have on an institution and the ways an institution can mitigate risks in these areas, strengthening systems and processes to

create a truly encompassing business continuity plan (BCP). With a large focus on cyber resilience, we explore ways to ensure data protection to safeguard your most critical asset. We also examine how an institution can support its community through a disaster, citing recommendations from the regulators themselves. Our hands-on tips and actionable intelligence makes sure you are asking the right questions to guarantee necessary planning.

Our secondary article this month reviews the Federal Reserve Board's (FRB) Semiannual Testimony from FRB Vice Chairman for Supervision Randal Quarles, providing insight into the agency's regulatory and supervisory goals. With a focus on transparency, simplicity and efficiency, the FRB plans to concentrate on supervisory rating systems, supervisory guidance, stress testing disclosures and Economic Growth, Regulatory Reform and Consumer Protection Act (EGRRCPA) implementation. Interestingly, we also monitor the role of vice chairman for supervision itself, as Quarles's tenure as the first official vice chairman proves effectual and could provide a path to future impact.

As always, Capco continues to monitor all relevant developments in risk and compliance. Please let us know how these areas are affecting your institution by reaching out to us at Capco.CRI@Capco.com. ❖

REGULATORY ROUNDUP

Regulatory and Compliance Alerts

HUD Issues Mortgagee Letter on Multifamily Housing and Guest Suites

On November 9, 2018, the Department of Housing and Urban Development (HUD) issued a [mortgagee letter](#) with best practice guidance to determine under what circumstances guest suites are permissible in multifamily rental, or cooperative projects with mortgages insured or held by HUD under the National Housing Act.

OFAC Releases Terrorist Assets Report

On November 7, 2018, the Office of Foreign Assets Control (OFAC) released its 2017 [Terrorist Assets Report](#). The report covers the nature and extent of assets that terrorism-supporting countries and organizations engaged in international terrorism hold in the U.S.

OCC Updates Enforcement Action Policies and Procedures Manuals

On November 13, 2018, the Office of the Comptroller of the Currency (OCC) issued revisions to its [Policies and Procedures Manual](#) for enforcement actions against institution-affiliated parties (IAP) of national banks, federal savings associations and federal branches and agencies of foreign banks. The manual generally sets forth the OCC's existing policies and procedures for taking enforcement actions against a current or former IAP in response to violations of laws, regulations, final agency orders, conditions imposed in writing or written agreements; unsafe or unsound practices; or breaches of fiduciary duty.

FinCEN Reissues Real Estate GTOs and Expands Coverage to 12 Metro Areas

On November 15, 2018, the Financial Crimes Enforcement Network (FinCEN) announced the issuance of revised [Geographic Targeting Orders](#) (GTOs) that require U.S. title insurance companies to identify the natural persons behind shell companies used in all-cash purchases of residential real estate. The purchase amount threshold, which previously varied by city, is now set at \$300,000 for each covered metropolitan area. FinCEN is also requiring that covered purchases using virtual currencies be reported.

FHFA Announces Maximum Conforming Loan Limits for 2019

On November 27, 2018, the Federal Housing Finance Agency (FHFA) announced that the maximum [conforming loan limits](#) for mortgages that Fannie Mae and Freddie Mac acquired in 2019 will increase. In most of the country, the 2019 maximum loan limit for one-unit properties will be \$484,350, an increase from \$453,100. In higher-cost areas, higher loan limits will be in effect.

OFR Publishes Annual Report on Risks to Financial Stability

On November 15, 2018, the Office of Financial Research (OFR) released its [2018 Annual Report](#) to Congress, stating that risks to U.S. financial stability remain in the medium range, reflecting a mix of high, moderate and low risks to the financial system. ❖

RESILIENCE THROUGH NATURAL DISASTERS

2018 proved to be an exceptionally difficult year for several areas in the U.S., from hurricanes and flooding on the East Coast to wildfires in the West. As communities rebuild from these disasters, financial institutions also have work to do.

Capco has received a number of questions and requests from clients across the nation dealing with natural disasters. It is critical that institutions are prepared for these types of events, in all aspects of business operations and people protection. It is also critical that institutions that suffer damages and losses, or have clients who suffer damages and losses, take the right steps to bounce back quickly, safely and securely.

Resiliency is key, and takes proper planning.

This means not only creating business continuity plans (BCPs) that address mission-critical operations, but also closely examining all potential risk factors to give your institution the ability to reconsider certain high-risk issues.

In order to ensure resiliency, it is essential to:

- Assess your risks
- Consider alternatives for high-risk issues
- Create a holistic BCP
- Communicate with staff to ensure understanding
- Protect your data

KNOW YOUR RISKS

In evaluating your institution's risk in the case of a natural disaster, it is critical to examine all aspects of the business, from physical locations and machinery to third-party vendor and client risk. Here are some areas many institutions need to consider more thoroughly when performing this assessment:

Physical Locations:

One of Capco's subject matter experts (SMEs) worked with a large Turkish cell phone service provider in 2009, and his team assessed that the company's main operations center was at risk for flooding. The team advised the company to move their operations center out of the designated 100-year flood plain, but executive management decided against the move. Two months later, a large flood swept through the center, destroying much of the hardware in the office.

While moving can be daunting, and there are many other factors to consider, such as employee relocation costs and potential rehiring, it is essential to find a balance that meets your organization's needs. In some situations, it might be prudent to transform a back-up operations site into the main operating site, as long as the business-critical aspects of the site are sufficient. For example, does the particular office need to be in a metropolitan area so that out-of-town clients or partners can easily visit? Will the office need a staff with particular skillsets, and is the office in an area where this type of staff can be found?

It is also important to keep in mind geographic risk factors when opening new branches. The one caution here is the importance of understanding whether a decision to not open branches in certain areas can be interpreted as "redlining," or cutting off certain populations from your services.

Physical Technology and Machinery:

While it may seem obvious to state the importance of understanding the risks associated with the hardware, machinery and technology certain offices within your institution utilize, it is common to view these risks in a silo, only considering the risks the machinery itself poses. In a site visit to a data center, a Capco SME found that the company housed their uninterruptible power supply (UPS system) in a cavity on the outside of the building.

The system's wet batteries (sulfuric acid batteries) were behind a metal door, and while there was a fan that turned on if the temperature in the enclosure reached a certain level, the assessment team found that the batteries were at risk of explosion if the temperatures rose above a certain temperature.

Now, place this data center in an area at risk for wildfires. A building that could potentially survive a wildfire is at far more risk when there are poorly enclosed wet batteries, as simply the spikes in temperature could set off an explosion. While in this scenario the problem was fixed before it was too late, it stands as an example of the importance behind understanding how your physical technology interacts with its physical surroundings and the risks they pose.

Third-party Risk:

When working with a third party, especially one that is essential to business-critical objectives, such as a data management provider, it is critical to understand their risks in the case of natural disasters as well. When deciding whether or not to partner with a third party, it may be prudent to examine their resiliency program. If there is something that does not feel secure enough, such as a main office located in a flood plain or an area at high risk for fires, your institution may decide to ask the third party to move locations, or provide supplemental contingency plans and security precautions.

Client Risk:

Clients, too, inherently bring risk to an institution. For many financial services institutions, one of the biggest areas for client risk in natural disasters lies in ensuring proper insurance. Many U.S. residents are still struggling through losses in the aftermath of this year's hurricanes, as well as storms from previous years. Tens of thousands of people have appealed to the Federal Emergency Management Agency (FEMA) for rebuilding funds, only to discover that though they qualify for small assistance payments, they did not have insurance sufficient to recover their major losses from the floods.

In the case that a property is valued above the federal maximum policy, but the owner is not required to have insurance above and beyond the federally-mandated insurance amount, the owner may decide not to pay for anything more. As flooding can damage or even completely destroy properties, lending institutions face additional problems and increase their credit risk exposure when they use these properties as collateral for loans.

One of the simplest and therefore most tempting solutions to protect the institution's portfolio is to not lend in certain areas. But, this type of lending behavior would most likely impact Equal Credit Opportunity Act (ECOA) and Community Reinvestment Act (CRA) efforts, as it could be seen as redlining.

Instead, your institution could try to balance your lending portfolio by lending in non-flood areas and finding lenders with secure collateral that will help offset these riskier types of lending. A strong strategic plan will facilitate safe and sound practices and help establish a diverse portfolio while still complying with ECOA and CRA. And, it is always a good idea to educate your customers on the risks they face if they are underinsured.

DEVELOPING A BCP

Once your institution has thoroughly assessed all areas for potential risk in the case of natural disaster, and reduced risk as appropriate, it is time to focus on the BCP. An effective BCP considers both short-term and long-term goals and objectives.

- **Short-term goals** are more tangible and relate to the immediate actions for ensuring that mission-critical functions are operating as usual so clients are not seeing any degradation in services. This includes mitigating problems; designating critical personnel and infrastructure; and recognizing the resources required for support.
- **Long-term goals** focus on more nebulous aspects of the BCP, such as recovery and restoration of facilities and full operations; re-alignment with third parties; consistent communications to personnel, clients and press; post-event assessment for lessons learned; and BCP modification.

Your institution should update its BCP after any significant changes to business operations; changes to technology infrastructure, third-party vendors; and/or gaps or shortcomings revealed through training or testing. The testing program for your BCP should be progressive, continuously increasing objectives and complexity to a point where the institution feels confident it can recover from an actual event. A BCP should include the following areas:



1. Personnel

An institution needs clear and defined tasks when it comes to personnel. By identifying which employees are integral to the BCP, an institution and its employees will be more prepared, which can shorten the recovery window. If this is not all identified beforehand, altering a policy during a natural disaster can be even more difficult.

- Host, at a minimum, **annual emergency trainings** to make sure identified personnel know their overall role in the recovery process.
- Have a **succession plan** in the case that someone cannot be reached, and have backup plans in the case that someone is unable or unwilling to return to work.
- Design a plan for **new accommodations for staff** in the case of substantial damage.
- Identify a **recovery team** to help displaced employees get up and running at their new location on recovered predefined critical business functions.

2. Communication

“Communication” in relation to a BCP covers communication with employees, emergency personnel, regulators, vendors and suppliers, customers and the media.

Prompt communication is critical, especially with employees and emergency personnel. Your institution should be able to reach all employees, even in isolated areas, and management should be aware of each employee’s evacuation plans.

The Federal Financial Institutions Examination Council (FFIEC) [Appendix G](#) states “emergency notification systems should be evaluated to determine their cost effectiveness.” One of the largest challenges, however, is ensuring accurate contact information for all employees.

Some effective models for employee notification include:

- Two-way polling phone system for confirming contact and message delivery
- Providing remote access to employees, including security measures like virtual private networks (VPNs)
- An ultra-forward service that allows incoming calls to be rerouted to a predetermined alternate location

A strong BCP will also allow an institution to facilitate conference calls and meetings between financial sector trade associations, financial authority working groups, emergency response groups and international exchange organizations to help with the recovery process. Determining the impact and operational disruptions across an institution’s regionalized industry is important.

Communication with Customers and the Media following a Natural Disaster

After a natural disaster, it is essential to ensure the safety of your firm's staff and operability of your business-critical objectives. However, it is also hugely important to have a plan in place for communicating with your customers and the media.

In the example of the Turkish cell phone provider, the flooding of their main operations center was just the beginning of their problems. After news was out that the center had flooded, two competing carriers immediately began offering consumers free mobile number porting to the competitors' networks if consumers were experiencing sub-par service. These ads started within 24 hours after the event, which resulted in significant losses to the impacted carrier.

When an institution contacts its customers and the media first, it has the upper hand in telling the story in a way that inspires trust and loyalty rather than fear and frustration. Letting your customers know what the damage is, what your plans are and how you are handling the setback could be the difference between losing your customers to the competition and creating long-lasting relationships.

It is advisable to have pre-developed statements to provide to the press, as well as focused communications to high-value clients.

3. Cyber-resilience

When a natural disaster occurs, it is essential that all critical business unit data is secure. Most institutions today rely on back-up servers or the cloud, so the loss of physical machines is not as catastrophic as it once was. But it is critical to ensure that the systems are always working properly and that there are policies and monitoring processes in place for continuous information backup and records storage.

Your institution must decide whether employees may work on personal computers after a natural disaster if they do not have a work-issued laptop or do not have access to something similar to a virtual private network (VPN). If employees are intended to work remotely and expected to access data, it may be prudent to require a multi-factor authentication system. Further, when identifying "critical" and "non-critical assets," an institution should pay attention to how they label their mobile, internet and telephone banking tools, as well as email capabilities.

In the event of a disruption, your institution's access to automated-teller systems may be limited, and using telecommunications to access bank accounts may become paramount. Along these lines, your institution should define automated tasks that can be performed manually if systems are inoperable. The BCP should outline things such as what duties employees can fulfill, the distribution of hard copy documents and reconciling general ledger accounts once systems are operational.

Taking Advantage of the Distraction: Cyberhacks during Natural Disasters

All the experts agree that the best way to defend yourself against a cyberattack is to think like the hacker. And it is not hard to see that the best time to attack someone is when they are already distracted. A natural disaster is the prime opportunity for a hacker to infiltrate your systems.

One of the most dangerous aspects of this type of attack could be that many hackers in this situation would decide to simply infiltrate and lay low for a while. Many institutions will be going through so much at the time of a natural disaster, including resetting systems, that an institution may not readily identify anomalous activities. In these cases, it could take months for an institution to notice a breach, as we have seen many times in the past.

It is therefore paramount that during and after a natural disaster, your institution strengthens controls for its systems and data. It could be beneficial to require another layer of multi-factor authentication during these times, and employees should have a clear understanding of cybersecurity protocol if primary physical locations are inoperable. Additionally, monitoring and surveillance should increase, to help detect any inappropriate access.

4. Recovery Facilities & Operational Bounce-back:

The FFIEC handbook also emphasizes the importance for financial institutions to have “formal arrangements for alternate processing capability in the event that their data processing site becomes inoperable or inaccessible.” Your institution must consider expectations based on size and complexity, and your impact on the overall financial system.

Some institutions may require same-day business resumption, however there may be circumstances allowing other financial institutions to respond less quickly. One important aspect of this is your institution’s level of reliance on third parties for access to data. Many institutions partner with vendors to house and secure data, so it is critical, when going through service level agreements, to make sure you look at where the third party’s physical locations are, and what their backup and resilience plans are.

The idea is that regardless of a disastrous event, your institution can continue business-critical operations. The question is: how does the institution operate on a day-to-day basis and how can you support that regardless of location? While the infrastructure of an institution — including physical branches, machinery, operations, procedures and more — is clearly important, in a natural disaster, the most essential piece becomes the data and how quickly and effectively you can access it.

Capco’s Cybersecurity and Resiliency Solutions practice can help your institution identify, prevent and detect process or technology failure — minimizing downtime and financial loss, protecting customers and preserving customer trust and your reputation in the face of natural disasters. Contact Scott.D.Ramsey@Capco.com to learn more about how we can help.



BEING THERE FOR YOUR COMMUNITY

Access to money during a disaster can be difficult and financial institutions should ensure they have plans in place to help people who need cash during an emergency.

With an increased reliance on access to payments electronically, disrupting events can make those systems inoperable. ATMs rely on systems to help validate withdrawal requests; and a disrupting event could impact electronic funds transfer systems. Financial institutions should therefore consider pre-established withdrawal limits for customers and alternative solutions, including sending payments to correspondent banks.

Institutions should also consider granting disaster loans to those who need it. In some cases, institutions may receive CRA [consideration](#) from their regulators for such loans. For example, the Office of the Comptroller of the Currency (OCC) gives special consideration for certain activities in communities designated by the federal government as major disaster areas (recognized under CRA as designated disaster areas (DDA)).

The OCC also issued [Bulletin 2012-28](#), which provides guidance for institutions in the event that a disaster could result in long-term or widespread disruption to critical services, and affect customers. The agency encourages institutions to consider:

- waiving or reducing ATM fees
- temporarily waiving late payment fees or penalties for early withdrawal of savings for affected customers
- working with borrowers who have been affected by the event by
 - restructuring borrowers' debt obligations, when appropriate, by altering or adjusting payment terms
 - expediting lending decisions when possible, consistent with safety and soundness principles
- reassessing the current credit needs of the community and helping meet those needs by originating or participating in sound loans to rebuild damaged property
- contacting state and federal agencies, as well as other financial institutions, to help mitigate the effects of the event

Through these disrupting events, your institutions should work with consumers, and be aware of regulations with requirements that change in the case of a natural disaster, such as Regulation Z (Truth in Lending Act), which provides consumers an option to waive or modify the three-day rescission period when a “bona fide personal financial emergency” exists.

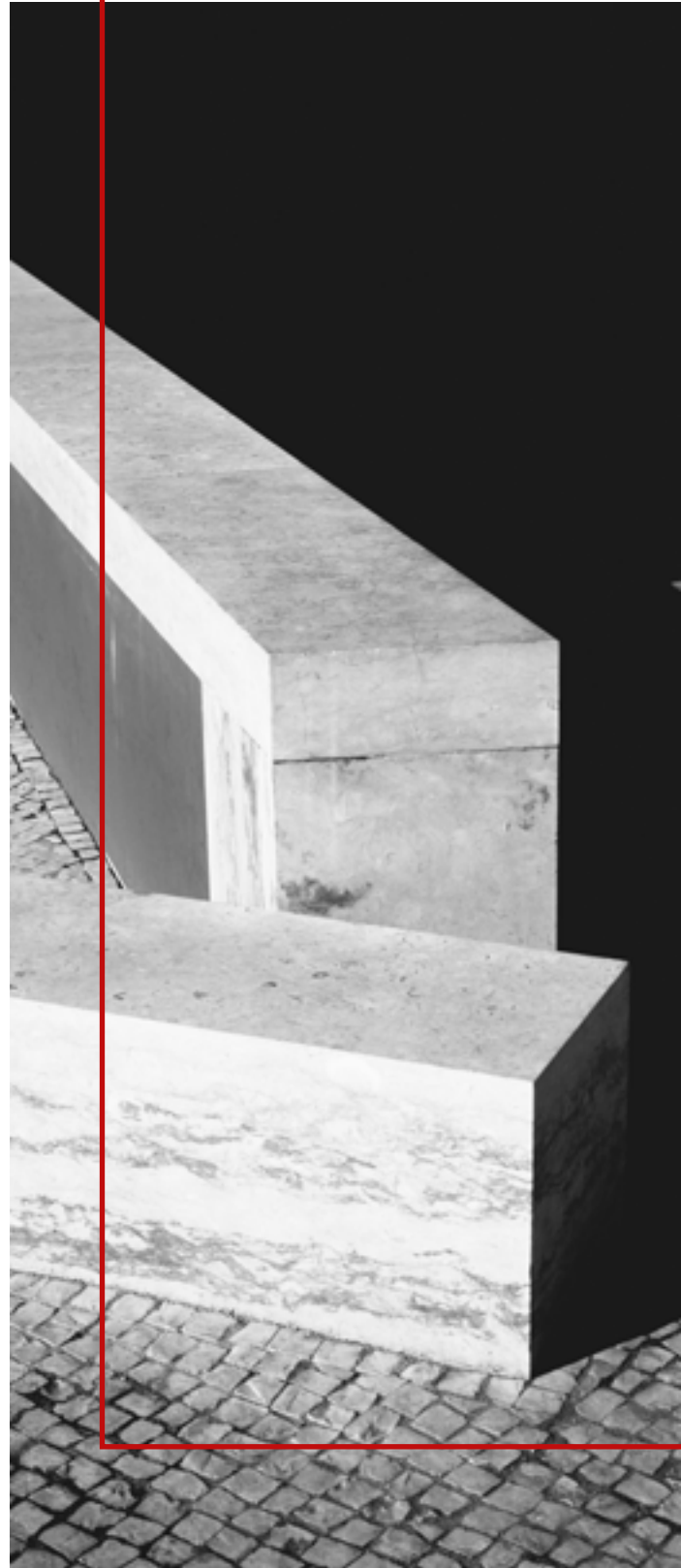
CONCLUSION

Regulators require a BCP that shows an institution's ability to maintain continuous operations, and the maximum tolerable downtime is now shorter than ever. Institutions need to provide for instantaneous recovery of time-critical business functions, and communities rely on financial service institutions in times of emergency.

Institutions must:

- Limit the magnitude of economic loss
- Minimize the extent of disruption to key business functions
- Minimize the likelihood of legal action against the organization or its officers and directors
- Identify and analyze the customer service and public image implications of extended service interruption
- Determine exposure to significant service interruption and design preventative measures
- Determine immediate, intermediate and extended recovery needs and resource requirements
- Minimize the number of decisions which need to be made at time of disaster
- Facilitate effective coordination of recovery tasks

An institution has the responsibility to protect the most important aspects of its functionality: its people and its data. Some of this comes from fully understanding the myriad of risks posed in the event of a natural disaster, and mitigating those risks where appropriate. However, only through proper planning and effective communication can an institution ensure resilience through disruptive events. As we move into 2019, it is critical to review your institution's business continuity policies and plans to guarantee preparedness in case of any natural disaster. ❖






CONGRESSIONAL HEARING SUMMARY: FRB SEMIANNUAL TESTIMONY

On November 15, 2018, Federal Reserve Board (FRB) Vice Chairman for Supervision Randal Quarles [testified](#) before the U.S. Senate Committee on Banking, Housing, and Urban Affairs for the FRB's semiannual testimony. Accompanying the verbal testimony, the FRB also [released](#) an inaugural Supervision and Regulation Report on November 9, 2018.

THREE OVERARCHING GOALS

Quarles' testimony and the report highlighted the FRB's efforts toward three goals in the agency's regulatory and supervisory efforts, both for regulated institutions and the public:

	Transparency
	Efficiency
	Simplicity

Exemplary of the agency's focus on these tenets, Quarles discussed several recent actions:

Supervisory Ratings Systems

The FRB [finalized](#) a new supervisory rating system for large financial institutions on November 2, 2018. In his testimony, Quarles said the new system will:

- Better align firms' ratings with their supervisory feedback
- Focus on issues most likely to affect safety and soundness

Supervisory Guidance

On September 11, 2018, the FRB, in conjunction with Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA) and Office of the Comptroller of the Currency (OCC) [issued](#) "Interagency Statement Clarifying the Role of Supervisory Guidance." The statement describes the difference between supervisory guidance and laws or regulations, and outlines ongoing agency efforts to clarify the role of supervisory guidance.

In his testimony, Quarles explained that supervisory guidance does not have the effect or force of a law, and agencies therefore do not take enforcement actions based on supervisory guidance. Quarles reinforced that this type of guidance clarifies agencies' expectations, priorities, views and opinions for how institutions should function in certain areas or with regard to certain laws or regulations. In line with the FRB's goals for transparency, supervisory guidance is intended to create consistency and clarity, and Quarles stated that Federal Reserve examiners will not treat guidance as legally enforceable.

Agencies' Efforts to Ensure Guidance is Non-binding

In efforts to ensure supervisory guidance functions as non-binding, "Interagency Statement Clarifying the Role of Supervisory Guidance" clarifies that regulatory agencies take ongoing precautions, such as:

- **Limiting the use of numerical thresholds** or other "bright-lines" in describing expectations in supervisory guidance (Numerical thresholds in guidance are exemplary and not required.)
- **Not criticizing an institution for a "violation" of supervisory guidance during an evaluation**, though examiners may sometimes reference supervisory guidance to provide examples of safe and sound conduct, appropriate consumer protection and risk management practices and other actions for addressing compliance with laws or regulations
- **Seeking public comment on supervisory guidance** to: improve the agencies' understanding of an issue; to gather information on institutions' risk management practices; or to seek ways to achieve a supervisory objective most effectively and with the least burden on institutions
- **Reducing duplication and overlap in supervisory guidance**
- **Clarifying the role of supervisory guidance** to examiners and institutions on an ongoing basis

Stress Testing Disclosures

The FRB has a set of proposed measures that the agency hopes will "increase visibility into the Board's supervisory stress testing program." The agency hopes these enhanced disclosures will provide:

- more granular descriptions of the models;
- more information about the design of scenarios; and
- more detail about the outcomes FRB projects, including a range of loss rates for loans held by firms subject to the Comprehensive Capital Analysis and Review (CCAR)

EGRRCPA IMPLEMENTATION

Of major concern in Quarles's testimony, and in the opening remarks of both Chairman Mike Crapo (R-Idaho) and Ranking Member Sherrod Brown (D-Ohio), were issues relating to the FRB's implementation of various aspects of the Economic Growth, Regulatory Reform, and Consumer Protection Act (EGRRCPA). The FRB has already taken several actions under EGRRCPA, including:

- Expanding eligibility of community banking firms for the Small Bank Holding Company Policy Statement, and for longer, 18-month examination cycles
- Giving bank holding companies below \$100 billion in assets immediate relief from supervisory assessments, stress testing requirements and some additional Dodd-Frank Act prudential measures
- Implementing changes to liquidity regulation of municipal securities and capital regulation of high-volatility commercial real estate exposures

One of the more pressing issues discussed during the hearing were two proposals under EGRRCPA the FRB announced on October 31, 2018, focusing on:

- [Changes](#) to applicability thresholds for regulatory capital and liquidity requirements
- [Prudential standards](#) for large bank holding companies and savings and loan holding companies

Community Financial Institutions

Crapo, in his opening statement, said, “These proposals are a step in the right direction, and I appreciate the Fed’s work to issue them quickly.” He also noted that the proposals included “a number of very positive changes to the current framework for regional banks,” including:

- Relief from advanced approaches capital requirements;
- A reduced liquidity coverage ratio;
- Changes to the frequency of supervisory and company-run stress testing; and
- In some cases, the disclosure of the results.

Brown expressed concerns, however, that the FRB’s proposals may provide more relief for larger banks, rather than smaller banks, as EGRRCPA implementation unfolds. Citing the FRB’s own report — which showed banks’ return on equity and average return on assets hit a 10-year high in Q2 2018, a 30 percent loan volume growth since 2013 and a 10-year low in the share of loans that are not performing — Brown argued that new legislations could undermine these developments.

Quarles noted, in addition to the aforementioned past actions the FRB has taken under EGRRCPA, that the agency, jointly with the FDIC and OCC, [issued](#) a proposal to reduce reporting requirements for small depository institutions. Under the proposal, only 63 percent of data items would be required in Q1 and Q3.

Foreign Banking Organizations

Both Brown and Crapo mentioned a need for more information regarding how the FRB plans to regulate and supervise foreign banking organizations (FBOs) within the U.S. financial system. Brown claimed the FRB was planning “rollbacks” for large foreign banks, which Brown asserted goes against the FRB’s progress report that said foreign banking organizations “continue to violate AML laws and skirt Dodd-Frank requirements.” In Crapo’s opening statement, he also acknowledged that the FRB has left FBO treatment largely unaddressed.

In his testimony, Quarles only mentioned FBOs in terms of U.S. involvement in forums such as the Financial Stability Board and the Basel Committee on Banking Supervision.

Potential Future Focus Areas

According to Crapo, the FRB still needs to focus on:

- Additional stress testing details, including CCAR
- Resolution planning
- Implementation of the community bank leverage ratio
- The provision that exempted cash deposits placed at central banks by custody banks from the supplementary leverage ratio

Quarles stated the FRB is working with the OCC and FDIC on a community bank leverage ratio proposal that is intended to reduce compliance burden for community banks.

THE FRB'S POWER MOVING FORWARD

With 2019's forthcoming split Congress, the rapid pace of legislative-driven regulatory reform we saw during 2018 is not likely to continue. While many of these issues are bipartisan, financial services reform moving forward will likely be at the agency level, and the FRB is going to play an important role in this process.

An interesting area to watch will be Quarles' position itself. The role of vice chair for supervision, created under section 1108 of the Dodd-Frank Act, had never been officially filled before Quarles took office in October 2017 (former FRB Governor Daniel Tarullo held the position on a de facto basis, appointed by former President Barrack Obama).

The Act [specifies](#) that "The Vice Chairman for Supervision shall develop policy recommendations for the Board regarding supervision and regulation of depository institution holding companies and other financial firms supervised by the Board, and shall oversee the supervision and regulation of such firms." Some [consider](#) this role to be one of the most influential positions in the U.S. banking industry.

Since Quarles took office, he has been thrust into the spotlight, delivering more speeches than the chairman or any FRB governor in 2018. While the semiannual testimony before the Banking, Housing and Urban Affairs Committee is statutorily mandated in the Dodd-Frank Act, he has additionally given numerous speeches and statements on the agency's behalf. Capco CRI will continue to monitor the announcements from the vice chairman for supervision as we move into 2019. ❖



ABOUT CAPCO

Capco is a global business and technology consultancy dedicated to the financial services industry, plus a dedicated energy division. Capco delivers innovative solutions in Banking & Payments, Capital Markets and Wealth & Asset Management, designed to withstand market forces, continual regulatory change and increasing consumer demand.

WORLDWIDE OFFICES

Bangalore	Frankfurt	Pune
Bangkok	Geneva	São Paulo
Bratislava	Hong Kong	Singapore
Brussels	Houston	Toronto
Charlotte	Kuala Lumpur	Tysons Corner
Chicago	London	Vienna
Dallas	New York	Warsaw
Dusseldorf	Orlando	Washington, DC
Edinburgh	Paris	

CONTACT US

Capco Center of Regulatory Intelligence
1101 Pennsylvania Ave., NW Suite 300
Washington, DC 20004
E: capco.cri@capco.com
P: 202.756.2263

@CAPCO [f](#) [t](#) [in](#) [v](#)

WWW.CAPCO.COM

© 2018 The Capital Markets Company NV. All rights reserved.

CAPCO