Banking on resilience: critical paradigm shift for Financial Service examiners

*The FFIEC's recent **release** of its Business Continuity Management handbook sets critical new paradigms for FS examiners, signaling a shift to operational resilience.*

Guidance from the Federal Financial Institutions Examination Council (FFIEC) makes it clear that, in the financial services industry, recovering IT systems quickly after an outage is no longer good enough.

Bank regulators are expanding the old business continuity planning/disaster recovery (BCP/DR) model to encompass all aspects of resilience — operational and cyber — effectively setting a new bar for regulated entities.

Rethinking Resilience

As FS regulators around the world shift their focus, PwC has **done the same**. We've been calling for a **rethinking of resilience** for a number of reasons:

- With globalization and increased competitive pressures leading to more outsourcing, offshoring, and automation, FS firms are now more interconnected and complex than ever before. A breakdown at any one step can disrupt the entire chain.
- Financial institutions are innovating in new areas — migrating more and more services and data to the cloud, for example — but managers' understanding of these technologies doesn't keep pace with the speed of change. They too often don't update their risk and, now, resilience programs to account for critical dependencies that emerge.

The FFIEC addresses these concerns and sets parameters for regulatory examiners of financial institutions and their third-party service providers.

Issued Nov. 14, the FFIEC's **Business Continuity Management** booklet represents the council's first significant update in more than four years. It expands its focus to business continuity ***management***, not just business continuity ***planning***. In doing so, it echoes some of the key tenets of the 2018 Bank of England's (BoE) influential discussion paper, **Building the UK financial sector's operational resilience**.

The update formalizes a definition of resilience found in the National Institute of Standards and Technology (NIST) Glossary: "The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate

- Enhanced risk management, stress testing, capital planning and liquidity management since the financial crisis have generally improved financial resilience. But traditional BCP/DR activities have received less attention in some firms, and often are focused on maintaining existing capabilities as opposed to continuously improving in maturity and depth.

- Regulators increasingly expect boards of directors to don the mantle of operational resilience oversight, a task for which they may not be adequately prepared.

attacks, accidents, or naturally occurring threats or incidents."

It also enjoins examiners to hone in on FS enterprises' and service providers' ability to keep their most important business functions operating and available to customers and other stakeholders. And it wants to see FS entities working to minimize any ripple effects an outage might have on others in its business ecosystem and on overall financial systems.

Subtle but significant shifts to resilience that the FFIEC will trigger

While the BoE's paper introduced bold new concepts, the 2019 FFIEC update appears to aim for a more nuanced pivot from BCP/DR to operational resilience.

Here are the shifts in a nutshell:

1. Moves emphasis away from BCP to BCM

Moves emphasis away from business continuity planning to business continuity management. The 2015 document spoke of systems *recovery*; the new booklet emphasizes the continuity of operations throughout the overall entity: technology, operations, testing, and communication, focusing on the "*continued maintenance* of systems and controls for the resilience of operations."

Let's talk

on building your organization's operational resilience >

The case for proactive action to build resilience

Resilience is taking precedence among FS regulators not only in the U.S. but worldwide. One reason is the escalation of cyberattacks on the FS industry, including nation-state sponsored incidents. Financial institutions globally experienced **six nation-state attacks alone** in 2018, up from two each in 2016 and 2017.

On the heels of its influential 2018 discussion paper, the BoE's decision to stress-test UK banks' operational resilience this fall prefigured the FFIEC changes. (The BoE plans to **publish the results** of those tests Dec. 10.)

But regulators already have been issuing resilience-focused Matters Requiring Attention (MRA) letters directly to financial institutions — even before the FFIEC published its update.

The writing is on the proverbial wall, and every financial entity and service provider would do well to pay attention. Those who embark now on the road to resilience will enjoy many advantages over those forced to contend with an MRA.

Remediating an MRA triggers a costly and stressful process of developing plans and implementing them on a tight schedule. Those so penalized must also satisfy regulators that they can maintain their resilience posture over the longer term, beyond remediation.

In the meantime, savvier organizations worldwide (those who scored high on resilience measures, so-called "high-RQ") have already been revamping their BC/DR programs with resilience in mind, according to PwC's **Digital Trust Insights study** on resilience.

Being proactive on resilience means being able to manage the scope, costs, and timing of building the organization's operational resilience.

Actions to take now

Lay the governance foundation for resilience | Set your recovery goals/targets | Measure your program's effectiveness | Stay current with changes

- Establish a team to oversee resilience enterprise-wide, ideally under the leadership of a Chief Resilience Officer.
- Step up your first-line (management) and business teams' involvement in responding to threats and disruptions.
- Revamp your remediation programs to include all affected functions: business units, operations, technology, RRP, and your resiliency organization.
- Take advantage of existing industry initiatives such as **Sheltered Harbor**, which

the **FFIEC booklet mentions** as “An example of an industry initiative to assist in addressing the resilience of customer account information.”

Contact us

Financial services

Adam Gilbert

Financial Services Advisory Regulatory Leader, PwC US

+1 (914) 882 2851

Email

Julien Furioli

Principal, Resilience Leader, PwC US

Email

Tamika Boateng

Financial services, PwC US

Email

Cybersecurity and privacy

Shawn Connors

Principal, Cybersecurity and Privacy, New York, PwC US

Email

Shawn Lonergan

Cybersecurity & privacy, PwC US

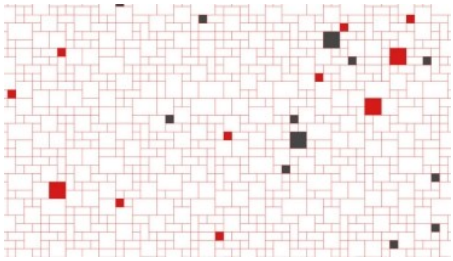
Email

Michael Hodges

Managing Director, Cybersecurity and Privacy, PwC US

Email

Related content

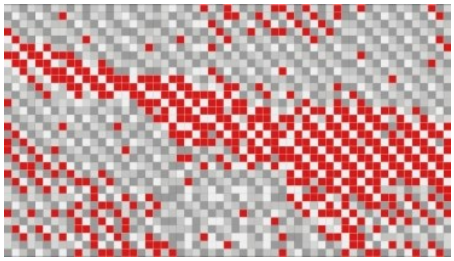


Digital Trust Insights: Raising the resilience quotient

Keeping data and operations running smoothly and securely while digital connections multiply is changing the face of resiliency, according to PwC's Digital

Operational resilience in Financial Services: Time to act

Joint report with TheCityUK to define and identify the key threats to operational resilience and recommendations to help ensure the UK remains a world-leader in...



Digital trust insights: Data trust pacesetters

Why it's time to shift to a data trust strategy, not just a data strategy. Focusing solely on the potential for value creation—how to use data to create new...

Follow us