



From Data Centers to Due Diligence

How DR Testing in Banks and Credit Unions Has Changed

Steve Carroll

Principal, BNP, Inc.

October 16, 2026

Table of Contents

Introduction	3
1997–2003: Annual tests of plans the institution ran itself	3
2008: Pandemic planning and a wider testing lens	4
2015: Testing moves to the service provider.....	4
Application environments: from owned data centers to the cloud	5
2019–2023: From recovery planning to resilience and third-party oversight.....	6
Recovery time frames now need a source.....	7
Conclusion: DR testing is now a third-party risk management discipline	8
References	10

Introduction

Disaster recovery (DR) testing in banks and credit unions began as a hands-on technical exercise: early federal guidance described tests that mobilized personnel at alternate sites and recovered systems there. Today most institutions run few of the systems they test. Their applications sit with core processors, software-as-a-service vendors and cloud providers, and the institution's role in a test is increasingly to obtain, review and challenge evidence from those third parties.

This article traces that shift through three decades of federal guidance and the data on how application environments have moved from owned data centers toward the cloud. Every regulatory statement and figure below is cited to its source; where data for banks and credit unions specifically is not available, the article says so.

1997–2003: Annual tests of plans the institution ran itself

In March 1997 the FFIEC revised its policy statement on [Corporate Business Resumption and Contingency Planning](#). It told senior management to ensure that "contingency plans are thoroughly tested at least annually" and that test results are reviewed. NCUA sent the same statement to credit unions as [Letter 97-CU-3](#) on April 7, 1997, adding that "each credit union should have a tested plan in place."

Third parties were already in view, but in a narrow role. An institution using a service bureau was told to "evaluate the adequacy of contingency planning and testing for its service bureau" and make its own plan "compatible" with the bureau's. The testing itself was still the institution's job.

The March 2003 FFIEC [Business Continuity Planning booklet](#), which replaced Chapter 10 of the 1996 IT handbook, set out four testing methods of increasing complexity:

1. Orientation/walk-through, "the most basic type of test."
2. Tabletop/mini-drill.
3. Functional testing, "the first type that involves the actual mobilization of personnel at other sites."
4. Full-scale testing, "the most comprehensive type of test."

The booklet expected recovery testing "at least annually" and warned that "unmanned recovery testing" was "not a sufficient test." Its emphasis was on the institution's own people, sites and systems. Even so, it added a line that foreshadowed what came later: "Even small, serviced institutions should participate in tests with their core service providers."

The same year, the Federal Reserve, OCC and SEC issued the [Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System](#) (April 8, 2003). It applied "most directly to the clearing and settlement activities of a limited number of financial institutions," so it shaped the largest firms more than community banks and credit unions.

2008: Pandemic planning and a wider testing lens

On March 19, 2008 the FFIEC agencies released an [updated Business Continuity Planning booklet](#) replacing the March 2003 original. The update "includes enhancements to the business impact analysis and testing discussions" and added key elements of the FFIEC's December 2007 Interagency Statement on Pandemic Planning.

The release also stressed that continuity planning matters whether an institution runs its systems in-house or "through third-party service providers." The guidance now explicitly covered systems that the institution did not operate itself.

2015: Testing moves to the service provider

In February 2015 the FFIEC added [Appendix J, "Strengthening the Resilience of Outsourced Technology Services"](#), to the BCP booklet. It named four areas: third-party management, third-party capacity, testing with third-party technology service providers, and cyber resilience.

The [February 2015 booklet's](#) examination procedures show how testing was being redefined. Examiners were asked to:

- "Determine whether testing with third-party providers is included in the institution's enterprise BCP testing program."
- "Determine whether the institution relies on proxy testing," defined as testing "conducted on like systems and with like interfaces" that is "sometimes used as a replacement for actual tests."
- "Determine whether management has received and reviewed testing results of their TSPs."
- Assess whether TSP contracts include elements such as "right to terminate language (if the TSP defaults on SLAs and RTOs)."

For many institutions the provider in question was a core processor, and that market is concentrated. A March 2024 [Kansas City Fed briefing](#) found that Fiserv, Jack Henry and FIS served over 70% of surveyed banks in 2022 and nearly half of surveyed credit unions in 2020.

Credit unions face an added constraint. Bank regulators can examine technology service providers, but NCUA "has no enforcement authority over third-party service providers"; its temporary authority under the Examination Parity Act of 1998 "expired on December 31, 2001" ([Atlanta Fed, January 2024](#)). The same article reports that a late-2023 ransomware attack on one provider disabled at least 60 credit unions, leaving roughly 100,000 members without digital account access for about three weeks.

Application environments: from owned data centers to the cloud

Public cloud hit 55% of enterprise workloads in 2025; trends point to 55–64% by 2030

Share of workloads, all industries (Flexera surveys; 19–20% of 2023–24 respondents were financial services).

No bank- or credit-union-only series exists; the one sector figure found (Treasury, 2021) is marked as a dot.

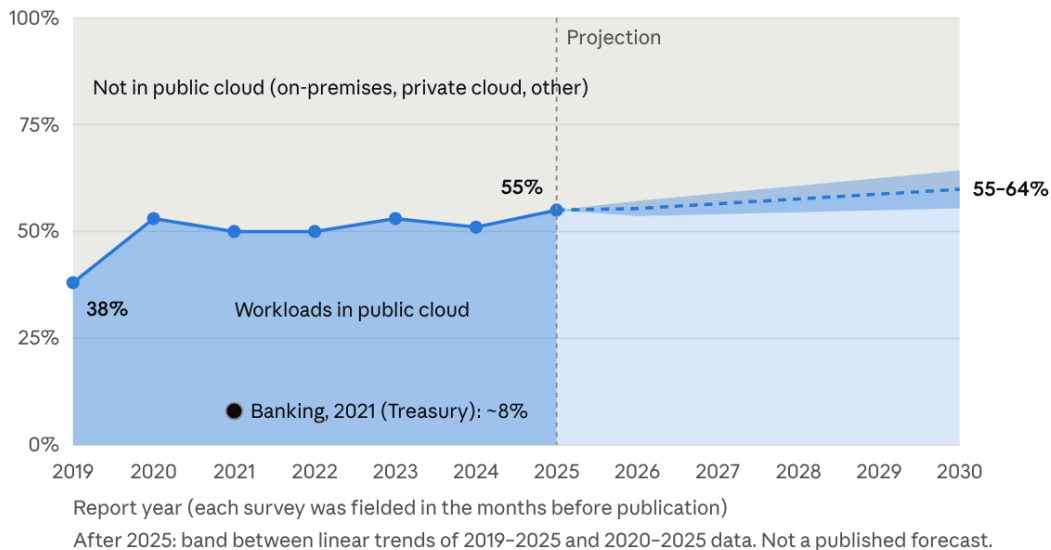


Figure 1. Sources: RightScale/Flexera State of the Cloud reports 2019–2025 (all industries, workloads in public cloud); banking dot: U.S. Treasury, Feb 2023, citing a 2021 survey. 2026–2030 is this article's linear-trend projection, not a published forecast. The remainder is everything not in public cloud and is not purely on-premises.

Across all industries, the share of workloads running in public cloud rose from 38% in Flexera's 2019 report to 55% in its 2025 report. The remainder is not purely on-premises: the 2019 report also put 41% of workloads in private cloud, which it noted may include virtualized environments that have been "cloudified." Flexera samples differ year to year, so small moves between reports should not be read as trends.

The 2026–2030 band is a projection made for this article, not a published forecast. It extends two straight-line trends through the Flexera data: the 2019–2025 trend, which includes the early jump, reaches about 64% by 2030; the flatter 2020–2025 trend reaches about 55%. For comparison, Flexera's 2025 respondents expected "an additional 6%" of workloads to move to public cloud within 12 months. Like the history, the projection covers all industries, not banks and credit unions specifically.

No consistent public series tracks this mix before 2019 or for banks and credit unions alone. Gartner's spending-based measure points the same direction: it estimated that 19% of addressable enterprise IT spending had shifted to cloud in 2018 ([Gartner, 2018](#)), and later put the figure at 41% in 2022 with 51% forecast for 2025 ([Gartner, 2022](#)). The two releases use different estimates, so they are cited here rather than plotted.

Banking has moved more slowly for core workloads but broadly for software. The [Treasury cloud report](#) cites a 2021 survey estimating that an average of 8% of banking workloads were cloud-based. It also reports:

- Over 90% of surveyed banks keep "at least some data, applications, or operations in the cloud," though only 5% described their use as mature.
- An ABA survey estimated banking SaaS adoption at "around 91 percent"; 43% of institutions with cloud deployments used PaaS and 29% used IaaS.
- Over two-thirds of surveyed banks want at least 30% of their applications and data in the cloud within three years.
- Many third-party suppliers have shifted to cloud-based offerings and no longer provide on-premises compatible solutions.

2019–2023: From recovery planning to resilience and third-party oversight

In November 2019 the FFIEC replaced the February 2015 booklet with the [Business Continuity Management \(BCM\) booklet](#). The OCC described the change as moving beyond the planning process to "enterprise-wide, process-oriented approaches" ([OCC Bulletin 2019-57](#)).

The [2019 booklet](#) changed testing in three ways that matter here:

- **Exercises versus tests.** "Exercises address people, processes, and systems whereas tests address specific aspects of a system." The methods are now full-scale, limited-scale and tabletop exercises, plus tests.
- **Frequency tied to risk.** Exercises and tests should occur "at appropriate intervals" or when new risks are identified, and plans "should be retested soon after" significant changes.
- **Third parties inside the program.** Section VII.I says third-party providers should be included in the enterprise exercise program based on their criticality, the right to test should be in the contract, and management should take part in provider tests, obtain results and remediation plans, and do its own analysis. "Any test results that affect the entity should be presented to its board." Section IV.A adds that review of a provider's BCM program "may include independent audit reports or SOC reports," and that "if management relies on SOC reports, it should verify whether business continuity activities are audited."

The booklet also recognized cloud recovery directly: "Cloud-based disaster recovery services may be considered as part of resilience programs," and it defines Disaster Recovery as a Service (DRaaS). In April 2020 the FFIEC followed with a [joint statement on cloud computing](#) stressing the "shared responsibilities between cloud service providers and bank clients."

On June 6, 2023 the Federal Reserve, FDIC and OCC issued the [Interagency Guidance on Third-Party Relationships: Risk Management](#), replacing the agencies' separate earlier guidance. NCUA is not a party to it. Its text places DR evidence squarely inside the third-party life cycle:

- **Due diligence:** determine whether the third party maintains "disaster recovery and business continuity plans that specify the time frame to resume activities and recover data," and review "the results of operational resilience and business continuity testing and performance during actual disruptions."
- **Independent reports:** consider reviewing "System and Organization Control (SOC) reports" and independent certifications.
- **Contracts:** require "operating procedures to be carried out in the event business continuity plans are implemented, including specific recovery time and recovery point objectives," and state "whether and how often the banking organization and the third party will jointly test business continuity plans."

The [Treasury Department's February 2023 cloud report](#) shows why direct testing is hard to obtain. It notes that "intensive in-person audits are challenging to accommodate at scale" for cloud providers, that "smaller financial institutions noted their lack of bargaining power," and that early adopters found it "particularly difficult to negotiate for audit rights." It also found that smaller institutions "tend to use cloud services largely through third-party software providers and managed service providers."

Recovery time frames now need a source

Auditors and examiners now frequently ask where an institution's recovery time frames came from. For cloud-based and SaaS systems, a stated RTO, RPO and, in some cases, MTD is treated as a claim, and the follow-up question is: what is the source? This is a field observation rather than a quoted examination procedure, but the published guidance points the same way.

The [2019 FFIEC BCM booklet](#) says recovery measurements "should be evaluated for alignment with third-party service providers' contracted recovery expectations" (Section III.A), that "management should verify whether the RTO is realistic," and that management should "verify such third parties' resilience capabilities" (Section IV.A). Its list of contract considerations includes the "capacity of third-party service provider to meet client recovery objectives in the agreements." The [2023 interagency guidance](#) expects contracts to provide recovery procedures "including specific recovery time and recovery point objectives," and due diligence on plans "that specify the time frame to resume activities and recover data."

The practical consequence is that banks and credit unions should not assign recovery time frames internally to systems they do not operate. The institution's business impact analysis sets what the business can tolerate. For a SaaS or cloud-hosted system, the RTO and RPO recorded in the plan should be the provider's documented commitment, cited to the document it came from. Where the provider's figure does not meet the business requirement, the booklet's answer is to "initiate an action plan and milestone(s) to document the situation," not to write in a better number.

Source of the figure	What to record with it
Contract, SLA or service schedule	Document name, section, effective date
Provider's business continuity or DR plan summary	Document name, version, date received
Provider's DR test results	Test date, scope, recovery times achieved
SOC report	Report period and whether business continuity was in scope; the booklet says to "verify whether business continuity activities are audited"

An RTO with no row in a table like this is the kind of number an examiner will now challenge.

Conclusion: DR testing is now a third-party risk management discipline

We are in a reality now where most DR testing in banks and credit unions uses third-party risk management (TPRM) techniques, not technical skills. No survey measures that share directly; the conclusion rests on the guidance trail and the data below.

Year	Guidance	What a "test" meant for the institution
1997	FFIEC policy statement; NCUA 97-CU-3	Test the institution's own plans at least annually; evaluate the service bureau's testing
2003	FFIEC BCP booklet	Walk-throughs through full-scale tests at the institution's sites; serviced institutions should join core provider tests
2008	FFIEC BCP booklet update	Enhanced testing discussion; plans cover in-house and third-party processing
2015	FFIEC Appendix J	Testing with TSPs, proxy testing and review of TSP test results become exam items
2019	FFIEC BCM booklet	Providers inside the exercise program; contract right to test; SOC report review
2023	Interagency TPRM guidance (Fed, FDIC, OCC)	DR and BCP evidence gathered through due diligence, contracts and monitoring

The data points the same way. Over 70% of surveyed banks run on one of three core providers ([Kansas City Fed](#)), and over 90% of surveyed banks keep at least some data, applications or operations in the

cloud ([Treasury](#)). When the system belongs to someone else, the institution's tools are the ones the 2023 guidance lists: due diligence on recovery plans, review of test results and SOC reports, contract terms for RTOs, RPOs and joint testing, and ongoing monitoring.

Technical skill has not disappeared. It has moved to the provider, and the institution's job is to verify it. For DR program owners, that means the core competencies are now reading a SOC report for business continuity scope, negotiating the right to participate in tests, and challenging a provider's results against the institution's own recovery objectives.

References

Regulatory guidance

1. FFIEC, [Corporate Business Resumption and Contingency Planning](#), revised March 1997 (FDIC copy).
2. NCUA, [Letter to Credit Unions 97-CU-3: Corporate Business Resumption and Contingency Planning](#), April 7, 1997.
3. FFIEC, [IT Examination Handbook: Business Continuity Planning booklet](#), March 2003 (FDIC copy).
4. Federal Reserve, OCC and SEC, [Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System](#), April 8, 2003 (SEC release).
5. OTS, [Financial Regulators Release Updated Business Continuity Planning Booklet](#), Press Release 08-011, March 19, 2008.
6. OCC, [Bulletin 2015-9: Strengthening the Resilience of Outsourced Technology Services \(Appendix J\)](#), February 6, 2015.
7. FFIEC, [Business Continuity Planning booklet, February 2015](#) (third-party hosted copy).
8. FDIC, [FIL-71-2019: Updated FFIEC IT Examination Handbook – Business Continuity Management Booklet](#), November 14, 2019.
9. OCC, [Bulletin 2019-57: Business Continuity Management booklet](#), November 14, 2019.
10. FFIEC, [Business Continuity Management booklet](#), November 2019 (third-party hosted copy; official version on [FFIEC IT Handbook InfoBase](#)).
11. OCC, [Bulletin 2020-46: FFIEC joint statement on cloud computing](#), April 30, 2020.
12. Federal Reserve, FDIC and OCC, [Interagency Guidance on Third-Party Relationships: Risk Management](#), 88 Fed. Reg., June 9, 2023 (final June 6, 2023).

Industry and market data

13. U.S. Department of the Treasury, [The Financial Services Sector's Adoption of Cloud Services](#), February 2023.
14. Alcazar, Baird, Cronenweth, Hayashi and Isaacson, [Market Structure of Core Banking Services Providers](#), Federal Reserve Bank of Kansas City, March 27, 2024.
15. Claire Greene, [Third-Party Risks and Credit Unions](#), Federal Reserve Bank of Atlanta, January 22, 2024.
16. RightScale/Flexera, [2019 State of the Cloud Report](#).
17. Flexera, [2020 State of the Cloud Report](#).

18. Flexera, [2021 State of the Cloud Report](#).
19. Flexera, [2022 State of the Cloud Report](#).
20. Flexera, [2023 State of the Cloud Report](#).
21. Flexera, [2024 State of the Cloud Report](#).
22. Flexera, [2025 State of the Cloud Report summary](#), March 19, 2025.
23. Gartner, [Gartner Says 28 Percent of Spending in Key IT Segments Will Shift to the Cloud by 2022](#), September 18, 2018.
24. Gartner, [Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025](#), February 9, 2022.