

Is Your BCM Program Trapped in an IT Structure?

Why BCM now needs a lane of its own, the symptoms to watch for, and where it can report so IT resources stay dedicated to IT

Steve Carroll

Principal, BNP, Inc.

November 19, 2026

Table of Contents

Introduction....3
BCM is not DR, and never was....3
Why BCM ended up in IT....4
What changed....4
What the guidance expects....5
Symptoms of a BCM program trapped in an IT structure....6
When it's time to restructure....7
Where should BCM live?....7
Making the move....8
Conclusion....9
Sources....9

Introduction

Is your Business Continuity Management (BCM) program trapped in an Information Technology structure? For many community banks and credit unions, the honest answer is yes, and for a long time it did not matter much. BCM grew up next to disaster recovery (DR), DR lived in IT, and the IT department was the natural home for both.

That is changing. As banking organizations scale up, and as the share of their applications delivered as cloud services keeps rising, structural cracks start to show when BCM reports up through IT. The work that matters most in BCM today looks less like restoring servers and more like third-party risk management and information security. A program organized around the data center will keep answering the questions of the last decade.

This is not a criticism of IT. Keeping systems running, secure, and current is a full-time job, and it keeps growing. When administrative risk duties are tacked onto that job, IT priorities are compromised, and so is the risk work. IT resources should be dedicated to IT. BCM is becoming equally important, but it runs in a different lane, one that calls for a different kind of effort: facilitating business units, analyzing vendors, and reporting risk to the board.

This article explains why BCM and DR are not the same thing, what the guidance says about where BCM belongs, what symptoms suggest your program is ready for a lane of its own, and how to decide whether to move it to enterprise risk management, operational risk, bank operations, information security, or third-party risk management. Where a point comes from published guidance, it is cited. Where it comes from BNP, Inc.'s own experience supporting banks and credit unions, it is labeled *Practice-based*.

BCM is not DR, and never was

Years ago, it was common to conflate business continuity with disaster recovery. The two overlap, but they answer different questions.

- **Disaster recovery** asks: if a system or site fails, how fast can we bring the technology back? It is owned by the people who run the technology.
- **Business continuity management** asks: if anything we depend on fails, can the business keep serving customers and members, and how long can it go without? It is owned by the business, with technology as one of many dependencies, alongside people, facilities, data, and outside providers.

The FFIEC drew this line clearly when it replaced its *Business Continuity Planning* booklet in 2019. It defines BCM as "the process for management to oversee and implement resilience, continuity, and response capabilities" (FFIEC BCM Booklet, 2019, Section I). It says the revised booklet focuses "on enterprise-wide, process-oriented approaches," and that BCM "should not be focused only on the planning process to recover operations after an event." Instead, "it should include the continued

maintenance of systems and controls for the resilience of operations" and "should be incorporated into the risk management life cycle of all systems, processes, and operations of an entity" (FFIEC BCM Booklet, 2019, Introduction).

That is not a description of an IT function. It is a description of an enterprise risk discipline.

Why BCM ended up in IT

Practice-based. There were good reasons BCM landed in IT, and it is worth naming them so the conversation about moving it does not become a criticism of IT.

- **The biggest risk used to be the data center.** When the core, the item processing, and the network all ran in a building the institution owned or leased, losing that building was the scenario that kept management up at night. DR was the heart of continuity, and IT ran DR.
- **IT had the project skills.** Recovery testing, backup rotation, and alternate site contracts are technical work. IT staff were often the only ones comfortable leading it.
- **Examiners asked IT.** BCM was examined as part of the IT examination, so it was natural for the person answering IT questions to answer BCM questions too.
- **It was a part-time job.** At a smaller institution, BCM was rarely a full-time role, and the IT manager or network administrator absorbed it.

None of those reasons was wrong at the time, and IT carried BCM well for years. What has changed is the kind of work BCM requires.

What changed

Practice-based. Three shifts have changed the kind of effort BCM requires.

The data center is no longer where the risk lives. Core processing, digital banking, loan origination, email, collaboration, document management, and payments increasingly run on platforms the institution does not own and cannot restore. When a hosted service fails, there is no server for IT to bring back. The recovery depends on the provider, and the institution's job is to keep the business running until the provider recovers. That is a third-party problem first and a technology problem second.

The most likely interruption is narrow but absolute. As we argued in *When Email Goes Dark*, the next interruption most banks and credit unions face is less likely to be a storm or a fire and more likely to be a complete outage of one service or one vendor, such as Microsoft 365. The building is fine, the staff are at their desks, and one critical dependency is simply gone. The FFIEC anticipates this. It warns that "A critical failure at a third-party service provider could have large-scale consequences" (FFIEC BCM Booklet, 2019, Section III.B).

Cyber events are continuity events. The FFIEC lists "cyber events, natural disasters, or man-made events" side by side as disruptions that "can interrupt an entity's operations" (FFIEC BCM Booklet, 2019,

Section I), and it expects that "management should identify cyber security risks" as part of the BCM risk assessment (FFIEC BCM Booklet, 2019, Section III.B). A ransomware event or a compromised vendor tests the continuity plan, the incident response plan, and the vendor contract all at once.

Put those together and BCM increasingly lives at the intersection of third-party risk management and information security. Neither of those usually reports to IT, and in a well-designed program, the risk functions are independent of the operations they oversee. That independence protects IT too. It lets IT spend its time on the systems, and lets someone else carry the risk analysis, vendor follow-up, and reporting that BCM now demands.

What the guidance expects

The guidance does not prescribe an organization chart. It does make clear that BCM is an enterprise responsibility and that it must be connected to the institution's broader risk management.

- **BCM covers the whole entity, including providers.** The board and senior management should "consider the entity's entire operations, including functions performed by affiliates and third-party service providers" (FFIEC BCM Booklet, 2019, Section II.A).
- **BCM integrates with enterprise risk management.** "BCM should integrate with an entity's enterprise risk management (ERM)," which "allows for the identification and management of risk across the entire entity." The level of formality "should be commensurate with the entity's complexity and risk profile" (FFIEC BCM Booklet, 2019, Section III).
- **Third parties are inventoried and their recovery is measured.** "Management should also inventory third-party service providers, including specific services they provide," and recovery measurements "should be evaluated for alignment with third-party service providers' contracted recovery expectations" (FFIEC BCM Booklet, 2019, Section III.A).
- **Responsibility does not move with the work.** The interagency third-party guidance states that "the use of third parties does not diminish or remove banking organizations' responsibilities" (Interagency Guidance on Third-Party Relationships, 2023, Section I).
- **Third-party due diligence is continuity work.** The same guidance expects banks to assess a provider's operational resilience, "including disaster recovery and business continuity plans that specify the time frame to resume activities and recover data," and to review "the results of operational resilience and business continuity testing and performance during actual disruptions" (Interagency Guidance on Third-Party Relationships, 2023, Section IV.C.2.i).
- **Third-party due diligence is also security work.** Due diligence "typically involves assessing the third party's information security program," including "its approach to protecting the confidentiality, integrity, and availability of the banking organization's data" (Interagency Guidance on Third-Party Relationships, 2023, Section IV.C.2.g).
- **Operational resilience ties the disciplines together.** The agencies' sound practices paper says "Robust operational risk and business continuity management anchor the sound practices," that "Secure and resilient information systems underpin the approach to operational resilience," and

that "Recognition of third-party risk is vital to operational resilience" (Sound Practices to Strengthen Operational Resilience, 2020, Introduction and Section 4).

- **Audit must be independent of BCM.** "Auditors should be qualified and independent of BCM processes" (FFIEC BCM Booklet, 2019, Section II.B).

Read together, these expectations describe a BCM program that is enterprise-wide, connected to ERM, and tightly linked to third-party risk and information security. A program can meet them from inside IT. But it asks IT staff to split their time between two demanding lanes, and that gets harder as the institution grows and moves more of its operations to the cloud.

Symptoms of a BCM program trapped in an IT structure

Practice-based. These are the patterns we see most often when BCM duties are layered onto an IT team's day job. None of them reflects poorly on IT. They are what happens when two demanding lanes share one set of people. One or two may be manageable. Several together are a signal.

1. **The BIA reads like a system inventory.** Resources are listed in detail, but business functions are thin, and impacts are described in technical terms rather than in customer, financial, or regulatory terms.
2. **Recovery times are best estimates.** Recovery time objectives for hosted applications are set internally without citing the provider's contract, service level agreement, or tested results.
3. **Testing means DR testing.** The annual test is a failover of the core or a backup restore. Business units have never exercised a scenario where a SaaS provider is down and nothing can be restored.
4. **Vendor management and BCM do not talk.** The vendor management program collects SOC reports and business continuity plans from providers, but nobody compares them to the BIA. The BCM coordinator could not say which critical functions depend on which critical vendors.
5. **Incident response and the BCP are separate documents with separate owners.** The information security incident response plan and the business continuity plan do not reference each other, and nobody has walked through a cyber scenario that triggers both.
6. **Business units see BCM as an IT request.** Department managers participate in the BIA as a request from IT rather than owning their own continuity strategies.
7. **One team designs, runs, and evaluates the program.** The people who run the recovery environment also write the BCM risk assessment and report the results to the board. However good the work is, independence is hard to show.
8. **Board reporting is a technical status report.** The board hears about backup success rates and test completion, but not about residual risk, risk appetite, or concentration in a handful of providers.
9. **IT priorities and risk work compete for the same hours.** IT is often a firefighting operation, and it should be: when a system is down or a patch breaks something, the fire is rightly the priority. But when BCM is tacked on as an administrative duty, risk work is what gives way. At the end of most

days, risk management is a can that gets kicked down the road. Both lanes lose: IT is pulled away from IT, and BCM waits.

When it's time to restructure

Practice-based. Symptoms tell you something is wrong. Triggers tell you the time to act has arrived. Consider restructuring when one or more of these occurs.

- **Your cloud footprint passes the tipping point.** When most of your critical business functions depend on applications the institution cannot restore itself, BCM has become primarily a third-party risk discipline, whatever the organization chart says.
- **The institution crosses a growth threshold.** A merger, an acquisition, a charter conversion, or asset growth that brings new examination expectations or a new regulator is a natural moment to revisit where BCM lives.
- **A core conversion or major outsourcing decision.** Moving from an in-house core to a service bureau, or from on-premises email to Microsoft 365, moves the recovery problem from IT to a vendor.
- **An exam finding or audit comment on independence or integration.** If examiners or auditors note that BCM is not integrated with ERM or third-party risk management, or that the same people design and evaluate the program, take that as a structural finding, not a documentation finding.
- **A real event exposed the gap.** If the last outage was a SaaS provider or a cyber incident and the business units had no plan for it, the program was built for a different kind of disruption.
- **The coordinator role turns over.** A vacancy is the easiest time to redefine the role and its reporting line, because no one has to give anything up.
- **ERM or operational risk is maturing.** If the institution has recently built or strengthened an ERM or operational risk function, BCM is one of the first programs that should plug into it.

Where should BCM live?

There is no single right answer, and the FFIEC expects the level of BCM and ERM integration to be "commensurate with the entity's complexity and risk profile" (FFIEC BCM Booklet, 2019, Section III). *Practice-based.* The table below compares the common homes for BCM. In every case, DR stays in IT, because restoring technology is an IT job. The question is who owns the program that tells IT what to restore, in what order, and what to do when restoring is not an option.

Home for BCM	Strengths	Watch for
Enterprise risk management	Puts BCM in the same risk inventory, appetite, and board reporting as every other risk. Best fit for the FFIEC's call to integrate BCM with ERM.	ERM may be thin at smaller institutions. BCM can become a reporting exercise if ERM lacks hands-on continuity experience.
Operational risk	Natural fit with process, people, systems, and external-event risk. Aligns with the operational resilience sound practices.	Some community banks and credit unions do not have a distinct operational risk function, so this may mean ERM in practice.
Information security	Strong link to cyber incident response, data integrity, and vendor security reviews. Often already independent of IT operations.	Can tilt the program toward cyber scenarios and away from people, facilities, and non-technical vendors. ISO workload is already heavy.
Third-party risk management	Directly addresses the narrow but absolute vendor outage. Connects BIA dependencies to due diligence, contracts, and monitoring.	Vendor management is often a contract and document function. It will need continuity expertise to evaluate recovery plans and test results.
Bank operations	Owns the business processes BCM protects, and is close to the customers and members who feel an outage. Often already coordinates branch and back-office continuity and manages core, payments, and card vendors day to day.	Operations is also a production function, so peak volumes can crowd out BCM. Make sure cyber and information security scenarios get equal weight with operational ones.
Information technology	Deep knowledge of systems and recovery. Workable at small institutions with mostly in-house systems.	IT's own priorities compete with administrative risk duties. Independence, business ownership, and third-party integration get harder as cloud dependence grows.

Practice-based. For most community banks and credit unions we work with, the strongest arrangement is BCM reporting into ERM or operational risk, with formal working links to information security and third-party risk management, and DR execution remaining in IT. Where ERM is not yet mature, bank operations and information security are both better fits than IT, and either one frees IT to focus on IT. Bank operations puts BCM with the people who own the business processes and feel an outage first. Information security is usually already independent of IT operations and already involved in vendor reviews.

Making the move

Practice-based. Giving BCM a lane of its own is an organizational change, and it goes better when it is treated as one rather than as a box moving on a chart.

1. **Separate the program from DR in writing.** Update the BCM policy and charter to define BCM as the enterprise program and DR as one of its components, owned and executed by IT.

2. **Name the new owner and the board reporting line.** Decide where BCM reports, who the coordinator is, and how results reach the board or its risk committee.
3. **Connect BCM and third-party risk management.** Map every critical business function to the vendors it depends on. Give the BCM coordinator a role in due diligence and annual reviews for critical vendors, and give vendor management a role in the BIA.
4. **Connect BCM and information security.** Cross-reference the incident response plan and the BCP, and run at least one exercise where a cyber event triggers both.
5. **Source the recovery times.** For every hosted application, record where its recovery time frame comes from: a contract, a service level agreement, a test result, or an internal assumption. Treat unsourced numbers as gaps.
6. **Re-run the BIA through a business lens.** Use the next BIA cycle to rebuild function-level impacts and dependencies with the business units as owners, not as interviewees.
7. **Test the scenario you are most likely to face.** Add a tabletop exercise for a complete outage of one critical SaaS provider, with no restore option, to the test plan.
8. **Keep IT close.** IT remains the most important partner in the program. The goal is to let IT resources stay dedicated to IT while BCM gets the dedicated effort it needs, not to create distance.

Conclusion

BCM did not end up in IT by mistake. It got there because, for a long time, continuity mostly meant recovering technology the institution owned. As banks and credit unions grow and move more of their operations to the cloud, that is no longer the main event. The disruptions most likely to test the program are outages and compromises at providers the institution depends on but does not control. Managing that risk is the work of third-party risk management, information security, and enterprise risk, with IT as an essential partner whose time is best spent on technology.

If several of the symptoms above sound familiar, and one of the triggers has arrived, it may be time to give BCM a lane of its own: a home that matches the risks it now manages, and that lets IT resources stay dedicated to IT.

Sources

1. Federal Financial Institutions Examination Council, FFIEC IT Examination Handbook: Business Continuity Management, November 2019, Introduction and Sections I, II.A, II.B, III, III.A, and III.B.
2. Board of Governors of the Federal Reserve System, FDIC, and OCC, Interagency Guidance on Third-Party Relationships: Risk Management, 88 FR 37920, June 9, 2023, Sections I and IV.C.2.

3. Board of Governors of the Federal Reserve System, FDIC, and OCC, Sound Practices to Strengthen Operational Resilience, October 30, 2020 (OCC copy, revised June 2026), Introduction and Section 4.
4. BNP, Inc., *When Email Goes Dark*, November 13, 2026.

Statements marked *Practice-based* reflect BNP, Inc.'s experience supporting banks and credit unions and are not drawn from the sources above.