



Business Continuity Planning Software Options for Financial Institutions

Market Overview, Strategic Considerations, and Emerging Technology Trends

Prepared by BNP, Inc.
Steve Carroll, Principal
May 2026

Disclaimer

This white paper is provided for informational purposes only and is intended to support strategic evaluation of business continuity planning software options. It does not constitute legal, regulatory, accounting, or technical advice. Financial institutions should apply their own governance, due diligence, and risk management processes when evaluating any platform or service model.

Executive Summary

Business continuity planning (BCP) software has evolved from a narrow plan management capability into a broader resilience technology category encompassing business impact analysis, dependency mapping, disaster recovery coordination, incident response, testing, third-party resilience oversight, and management reporting.

For financial institutions, platform selection increasingly reflects not only operational requirements, but also regulatory expectations, governance maturity, and long-term resilience strategy. Today's market includes several distinct solution models: bank-focused continuity platforms designed for examiner readiness and simplicity; enterprise resilience platforms with more advanced operational capabilities; GRC-centered platforms that embed BCM within a wider risk and compliance ecosystem; and adjacent service models that incorporate continuity capabilities into vendor risk or managed service offerings.

Each model presents tradeoffs across implementation effort, flexibility, integration depth, and strategic alignment. At the same time, AI-enhanced BCM and incident response capabilities are emerging as a potentially disruptive force, offering meaningful potential to improve data maintenance, dependency analysis, incident detection, and response coordination while introducing new governance and oversight considerations.

BNP Insight

Institutions are better served by prioritizing strategic fit, governance sustainability, data ownership, and long-term adaptability over feature completeness alone.

Market Context and Regulatory Drivers

Regulatory and Supervisory Expectations

Financial institutions face sustained supervisory expectations to maintain a living, tested, and board-governed continuity management program rather than a static recovery plan. This has increased demand for software platforms that help institutions support governance, maintain current information, demonstrate oversight, and evidence more defensible continuity processes.

A Broadening Resilience Challenge

At the same time, the resilience challenge has expanded. Business continuity software is no longer evaluated solely on its ability to store plans or maintain contact lists. Institutions increasingly require visibility into process interdependencies, technology dependencies, vendor concentration risk, cyber-related disruption scenarios, and the practical coordination required to respond to operational incidents.

These pressures are pushing the market beyond traditional BCP repositories and toward more integrated resilience, incident response, and operational coordination capabilities.

Examiner Consideration

A platform that improves defensibility, repeatability, and governance evidence is often more valuable than one that simply expands feature breadth.

Overview of BCP Software Categories

The BCP software market for financial institutions can be grouped into several functional categories:

- **Bank-Focused Continuity Platforms** — Emphasize examiner readiness, straightforward business impact analysis, plan maintenance, and usability for smaller or mid-sized institutions.

- **Enterprise Resilience Platforms** — Provide more advanced capabilities for dependency mapping, incident coordination, scenario analysis, and operational resilience management, often with greater implementation complexity.
- **GRC-Based Platforms** — Embed BCM within a broader framework that may also include enterprise risk management, compliance, audit, policy governance, and third-party oversight.
- **Adjacent Service Models** — Deliver continuity capabilities through managed service providers, advisory-led platforms, or third-party-risk solutions with continuity modules.

Interpretive Discussion of the Current Market

Several themes help clarify why different institutions select different solution models and why software selection is increasingly intertwined with resilience strategy, operating model design, and vendor risk considerations.

- Bank-specific BCM platforms continue to emphasize examiner readiness and simplicity, particularly for community and smaller regional institutions.
- Integrated service-oriented providers can improve operational efficiency by combining BCM, IT, and disaster recovery capabilities, while potentially increasing concentration risk.
- GRC-centric platforms appeal to institutions seeking a single system for BCM, enterprise risk, compliance, or policy management.
- Third-party-risk-anchored approaches align continuity more closely with vendor dependency management.
- AI-enhanced BCM and incident response solutions are emerging as a category of interest where institutions want faster detection, dynamic dependency insights, AI-assisted plan maintenance, and more automated response coordination.

Market Shift

Software selection is now a strategic decision tied to operating model, data architecture, and future resilience capability. A comparison of feature checklists will not settle it.

Low-Code / No-Code Platforms and the BCMaaS Model

A notable model is the use of low-code and no-code development platforms, most prominently Microsoft's Power Platform, combined with enterprise collaboration tools to deliver BCM capabilities outside of traditional packaged software.

This architecture supports two distinct delivery models. For smaller institutions, it enables a Business Continuity Management as a Service (BCMaaS) approach in which a specialized provider designs, implements, and maintains the BCM program using configurable tools embedded within the institution's own environment. For larger or more technically mature organizations, the same platform stack can support a largely in-house BCM capability owned and maintained by internal teams.

A key structural advantage of this approach is data ownership and control. Unlike traditional multi-tenant SaaS products, a Power Platform solution can operate within the institution's own Microsoft 365 environment, allowing direct integration with AI services such as Azure OpenAI or Microsoft Copilot without dependency on a vendor-controlled roadmap or cross-tenant constraints.

Strategic Advantage

For institutions already operating in the Microsoft 365 ecosystem, internally controlled low-code architectures can create a practical path to BCMaaS delivery, tighter workflow integration, and more direct AI utilization, provided that governance and technical support are sufficient.

Selection Considerations for Financial Institutions**Prioritizing Strategic Fit**

Institutions should prioritize strategic fit rather than feature volume. Smaller banks may value speed, examiner-ready outputs, and low administrative burden, while larger or more complex organizations may place greater importance on integration, dependency mapping, resilience analytics, or incident coordination.

Governance and Due Diligence

Software selection should be supported by a governance and due diligence process that evaluates data quality expectations, implementation effort, ongoing maintenance burden, reporting needs, internal ownership, access controls, cyber considerations, and third-party concentration risk.

Data Architecture and AI Utilization

Data architecture is now a material consideration. Multi-tenant SaaS environments may constrain how institutions use their own continuity data for AI or external analytics, whereas internally controlled environments can provide greater flexibility for integration, export, modeling, and oversight.

Practical Standard

Successful implementations are less often defined by selecting the most feature-rich platform and more often by selecting a solution that the institution can realistically govern, maintain, and integrate over time.

AI-Enhanced BCM and Incident Response as an Emerging Technology

AI-enhanced BCM and incident response platforms represent a shift toward more dynamic resilience capabilities. Recent market commentary suggests movement away from static, manually maintained continuity plans toward approaches that use AI to support predictive risk identification, faster incident detection, automated workflow routing, and more continuously updated recovery information.

Most Relevant Use Cases for Banks

- AI-assisted business impact analysis and data synthesis
- Automated or semi-automated mapping of interdependencies across processes, applications, vendors, and facilities
- Earlier recognition of operational or cyber-related disruptions
- Guided incident response actions and scenario support during crises

Governance Considerations

These tools should be treated as an emerging technology rather than a mature replacement for foundational BCM discipline. Financial institutions should expect increasing emphasis on model governance, validation, data quality, explainability, cybersecurity integration, human oversight, and documented accountability for the use of AI outputs in continuity and incident response activities.

Emerging Risk

Near-term opportunities may be strongest in administrative acceleration, data synthesis, scenario support, and incident coordination rather than fully autonomous decision-making.

Strategic Implications of AI for BCM

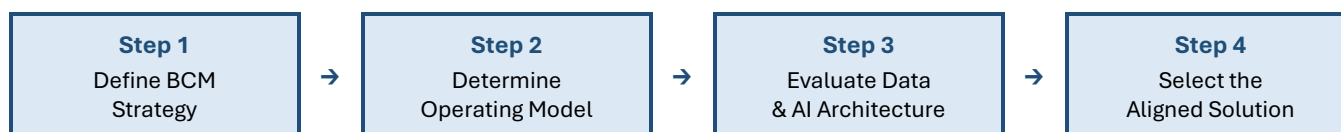
For banks, AI in BCM is a strategic question for management and the board, with consequences well beyond any single product feature. If these capabilities mature, they could materially change how institutions maintain continuity data, identify disruptions, coordinate response actions, and allocate resilience resources.

- BCM programs may become more dynamic and data-driven over time.
- Institutions may need to integrate BCM more closely with cybersecurity, IT operations, third-party risk management, and enterprise risk management.
- Governance expectations are likely to increase in areas such as model oversight, validation, auditability, access control, and defined human decision rights.
- Vendor selection may increasingly favor platforms with stronger data integration, analytics, operational resilience support, and practical AI-enabled capabilities.

A prudent strategic posture is to monitor the market closely, pilot targeted use cases, and expand adoption gradually while preserving accountability, transparency, and control.

Decision Framework for Financial Institutions

The framework below is intended to help institutions move from generic software comparison to a more defensible decision process grounded in strategy, operating model, data architecture, and governance.



- Define the program objective first: examiner-ready plan management, broader operational resilience, integrated risk management, or a managed-service model.
- Determine whether the institution wants a packaged SaaS product, BCMaaS delivery, or an internally owned low-code platform capability.
- Assess how the platform's data model affects integration, reporting, and future AI utilization, including whether data remains within the institution's environment or a vendor-controlled architecture.
- Select the solution model that aligns with the institution's size, complexity, governance capacity, and long-term resilience roadmap.

Comparative Overview of Representative BCP Software Options

The following table provides a directional comparison of representative BCM solutions and adjacent delivery models relevant to financial institutions. It is intended to support strategic shortlisting and due diligence rather than serve as an exhaustive market ranking.

Vendor	Primary Offering Type	Target FI Segment	Deployment Model	Strengths for Banks	Key Considerations / Limitations
Safe Systems – BCP Blueprint	Standalone BCM system	Community banks	SaaS	FFIEC-aligned, examiner-ready structure; widely used in community banking	BCM-only focus; limited ERM integration

Vendor	Primary Offering Type	Target FI Segment	Deployment Model	Strengths for Banks	Key Considerations / Limitations
Fusion Risk Management	Enterprise BCM / operational resilience	Mid-size & large banks	SaaS	Deep BIA, dependency mapping, resilience and crisis management	Higher cost and complexity
RSA Archer (Business Resiliency)	BCM within GRC / IRM platform	Banks using Archer GRC	SaaS	BCM integrated with ERM, audit, vendor risk	Heavy configuration and admin overhead
Riskconnect	Enterprise risk & resilience platform	Mid-size banks	SaaS	Combines BCM with operational risk and resilience reporting	Less FI-specific content out of the box
MetricStream	GRC platform with BCM module	Larger or complex banks	SaaS	Strong governance, compliance, and scalability	BCM is one module among many; meaningful implementation effort
Castellan Solutions	BCM & operational resilience specialist	Banks & regulated entities	SaaS	Strong scenario testing and resilience modeling	Smaller footprint in community banking
Continuity Logic	Standalone BCM software	Small-mid banks	SaaS	Practical BIA, plan management, testing	Limited ERM integration
Preparis	Lightweight BCM & crisis management	Small banks	SaaS	Ease of use; faster implementation	Less depth for complex environments
Tandem (CoNetrix)	BCM / DR planning & advisory platform	Community banks	SaaS	Banking-focused continuity and disaster recovery expertise; strong advisory support	More consulting-driven; less ERM breadth than large GRC tools
nContinuity (nContracts)	BCM module within vendor risk platform	Banks using nContracts	SaaS	Tight integration with third-party risk management and contracts	BCM depth depends on broader nContracts configuration
OnSpring	Configurable GRC / BCM platform	Banks & regulated organizations	SaaS	Highly configurable workflows; BCM integrated with risk & compliance	Requires configuration effort; fewer banking-specific defaults
NAVEX	GRC platform with BCM / resilience capabilities	Mid-size & large regulated entities	SaaS	Strong governance, policy, and compliance integration	BCM not core focus; may exceed the needs of smaller banks

Use of the Table

This comparison is directional rather than exhaustive. Institutions should validate current capabilities, deployment approaches, pricing, implementation requirements, and strategic fit during due diligence.

Conclusion

The BCP software market for financial institutions now spans a broad range of solution models, from focused continuity management tools to integrated resilience and GRC platforms. No single model is universally superior; the appropriate choice depends on institutional size, complexity, governance maturity, integration needs, and long-term resilience objectives.

At the same time, the rise of AI-enhanced BCM capabilities and alternative platform models, including BCMaaS and low-code architectures, suggests that the market is entering a new phase. Beyond documentation and testing, software may increasingly support ongoing analysis, coordination, and decision support.

Bottom Line

Financial institutions that approach software selection through the lens of strategic fit, governance sustainability, and data ownership are more likely to strengthen resilience without creating unnecessary complexity or control gaps.

Disclaimer

This white paper is intended to provide a strategic discussion of software categories, selection considerations, and emerging technology trends relevant to business continuity planning for financial institutions. It does not constitute legal, regulatory, accounting, cybersecurity, or technical implementation advice. Institutions should perform their own due diligence and align decisions with their risk appetite, governance structure, contractual standards, and applicable supervisory expectations.