White paper

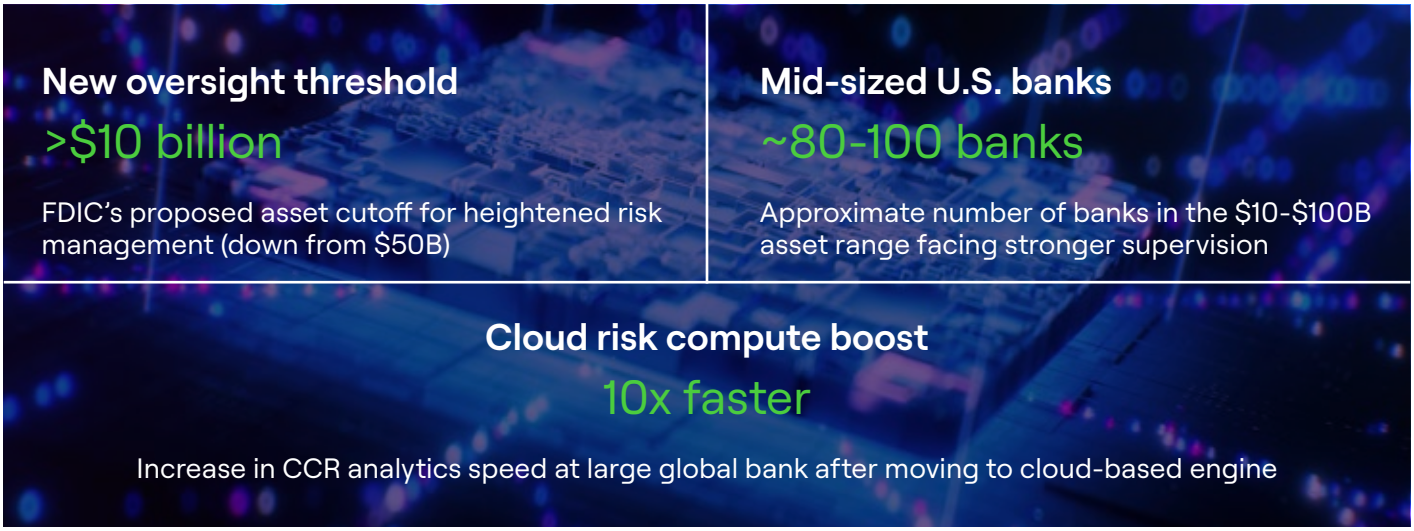
Navigating heightened regulatory pressures on U.S. mid-sized banks

Unlock resiliency with robust counterparty risk management

Introduction

Mid-sized U.S. banks are entering a new era of heightened regulatory scrutiny and risk management expectations.

In the aftermath of several high-profile bank failures in 2023, regulators are lowering the threshold for "big bank" standards to include regional banks. This shift means that banks in the $10B–$100B range, which previously enjoyed lighter oversight, must now upgrade their counterparty credit risk (CCR) management to meet more rigorous standards.



The challenges of CCR

CCR refers to the risk that a counterparty (e.g., a borrower, trading partner or derivative counterparty) could default on its financial obligations, potentially causing losses to the bank. Robust CCR management entails accurately measuring exposures (especially on derivatives and off-balance sheet contracts), setting prudent limits, securing adequate collateral and preparing for stress scenarios.

While mid-sized institutions tend to have less complex portfolios than Wall Street mega-banks, they are not immune to CCR challenges. Many provide derivatives to clients and engage in interbank transactions, creating a network of counterparty exposures. Traditionally, their risk systems have been simpler and more siloed, often focusing on loan credit risk and basic metrics for derivatives. Now, however, regulators expect mid-sized banks to adopt sophisticated CCR practices on par with far larger banks. This comes at a time when market volatility, geopolitical events, and emerging risks like climate impacts are testing the resilience of all banks' risk management and ability to keep their capital hard at work.

How to enhance your approach to CCR

Fortunately, advances in technology – especially cloud-based risk analytics platforms – offer mid-sized banks a cost-effective path to enhance CCR capabilities. Modern CCR systems can be delivered via the cloud with robust security and give regional banks access to powerful analytics without needing a massive on-premise infrastructure.

By leveraging these technologies and strengthening governance, mid-sized banks can not only meet new regulatory requirements but also better safeguard themselves against counterparty defaults that could threaten their stability.

Read on to discover:

- Which banks are affected
- What their CCR needs are
- How they can build robust CCR frameworks
- The role of secure cloud-based solutions

Heightened regulatory scrutiny

Regulatory changes are pulling mid-sized banks into a stricter oversight regime.

In 2018, the Economic Growth, Regulatory Relief, and Consumer Protection Act had relaxed many "big bank" regulations for institutions with less than $100B–$250B in assets. Banks in the $10B–$50B range, for example, were exempted from certain risk management requirements that larger banks faced.

However, lessons from the bank failures of March 2023 (such as Silicon Valley Bank and Signature Bank) have prompted regulators to reverse course. In October 2023, the FDIC proposed new guidelines that extend robust governance and risk management standards to all banks with over $10 billion in assets. Under these proposed rules, banks with $10B+ in assets must implement "large bank" risk management practices including: having a Risk Committee of the Board, appointing a Chief Risk Officer, conducting comprehensive risk assessments, and adhering to detailed guidelines on everything from liquidity risk to credit risk management.

This is a dramatic lowering of the threshold, and it effectively treats a $10B regional bank more like a $100B+ institution in terms of expected risk controls. In fact, the FDIC guidelines draw from the Fed's prior guidance for $100B banks, but in some areas, they go even further. For banks $10B–$50B (which have never had heightened standards), this is a significant new compliance burden. Even banks $50B–$100B (which briefly had higher standards pre-2018) will face more detailed requirements than before.

Moreover, regulators have made clear that while these expectations will apply proportionally based on size and complexity, even the smaller end of this spectrum must upgrade practices relative to their historical norms. Notably, the FDIC justified the broader scope by explicitly noting that recent failures revealed shortcomings in risk management at banks well below the old $50B level. Likewise, the Federal Reserve and OCC have signaled support for tougher standards on smaller regionals.

2018: Regulation relief

Threshold for enhanced supervision raised from $50B to $250B. Banks under $100B saw many big ban rules lifted.

Mar 2023: Mid-sized bank failures

Collapse of 3 regional banks (SVB, Signature, First Republic) reveals oversight gaps. Regulators re-evaluate standards.

Oct: 2023: FDIC proposal

FDIC proposes applying large-bank governance and risk management standards to all banks >$10B in assets.

Aug 2023: Capital rule changes

Fed/Basel propose higher capital and new risk calculations for banks >$100B. Banks get until 2028 to fully comply.

2024-2025: Implementation

Finalization of rules and phased implementation. Banks >$10B are expected to build up risk functions before deadlines.

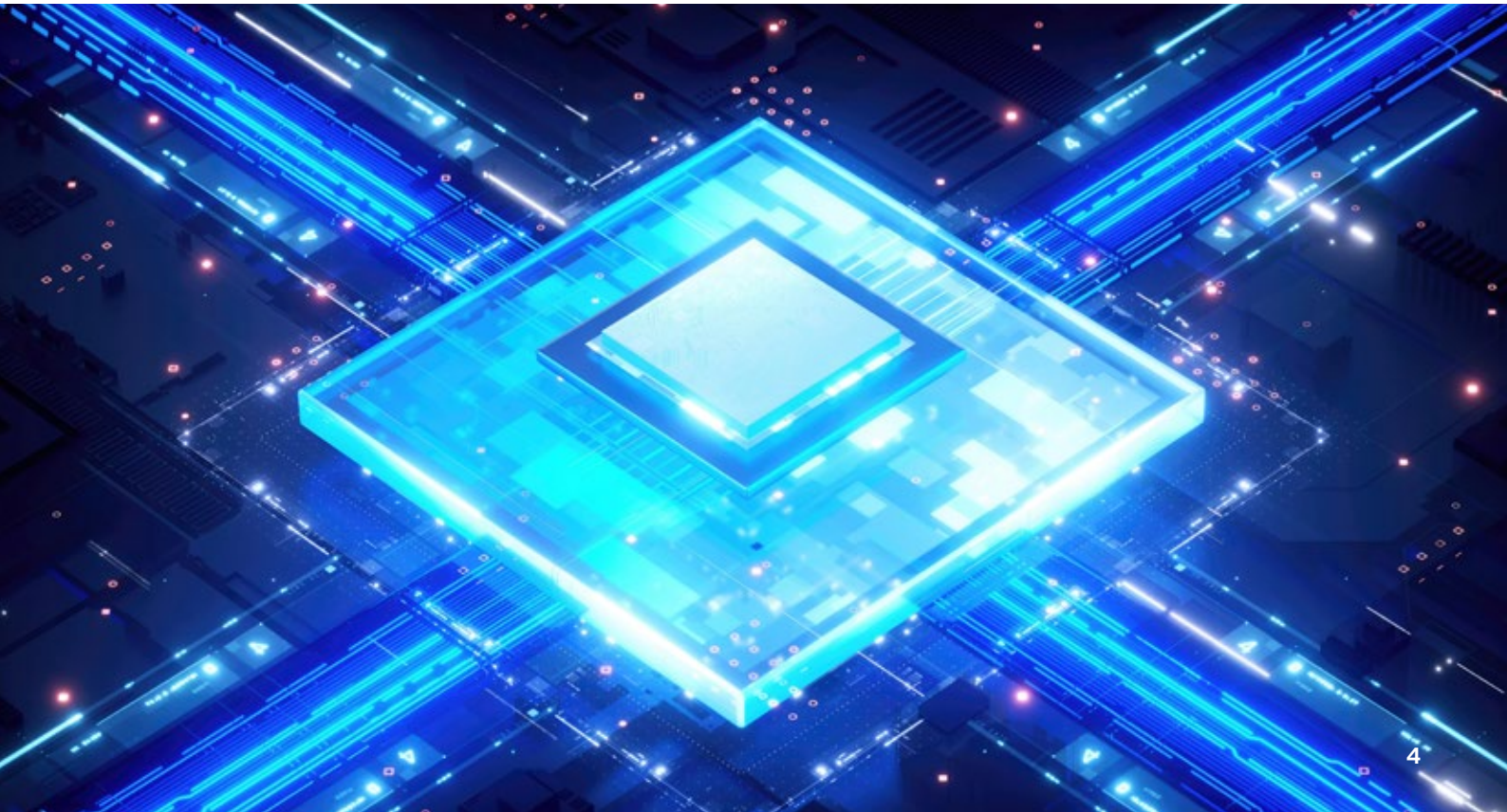
Beyond governance, regulators are revising technical capital rules that directly impact counterparty risk management. In July 2023, U.S. agencies unveiled the Basel III Endgame capital proposals, which, among other things, would apply the standardized approach for CCR (SA-CCR) universally for calculating derivatives exposure, and introduce a new capital charge for credit valuation adjustment (CVA) risk for banks above $100B in assets. Previously, only the very largest banks were required to use these sophisticated measurements, while mid-sized banks often used simpler methods.

Moreover, under the proposal, by 2028 banks with assets of $50–$100B must also adopt these advanced approaches. This means mid-sized banks will need systems that can compute complex exposure measures – a notable change from the simpler Current Exposure Method many used historically.

The Federal Reserve estimates these changes will raise overall capital requirements by ~16%, with especially large impacts on some regional banks' required capital. In practical terms, mid-sized banks will have to hold more capital against counterparty exposures and demonstrate to examiners that they can rigorously measure those exposures.

The takeaway: All signs point to a tougher supervisory regime: stronger risk governance, more granular risk data and higher loss absorbency. In response, mid-sized banks' boards and management are already beefing up risk functions. They are hiring experienced risk officers, forming board risk committees and investing in better analytics.

Regulators have made it clear that proactive investment in compliance efforts now is far preferable to remedial action later. And as FDIC Chair Martin Gruenberg noted, effective risk management should be right-sized to a bank's risk profile, regardless of asset size. For mid-sized banks, CCR is one such area coming into focus, given their growing portfolios of derivatives and off-balance-sheet exposures. But what does CCR actually entail for these banks, and why do they need to shore it up?



Counterparty credit risk needs and challenges

CCR is the risk that a counterparty to a financial contract defaults before fulfilling its obligations, forcing the bank to replace or write off the contract at a loss.

For mid-sized banks, CCR primarily arises from derivatives (swaps, forwards, options) and certain loan commitments or securities financing transactions. While these banks are not trading at the scale of JPMorgan or Goldman, many have meaningful derivatives books. For example, a $50B regional bank might offer interest rate swaps to its commercial borrowers to help hedge rate fluctuations, or foreign exchange forwards to local exporters. The bank often offsets those client trades with larger dealer banks, but it retains the credit exposure to each counterparty in the chain – the client and the dealer (or central clearinghouse if cleared).

So, what do mid-sized banks need in relation to CCR?

Accurate measurements of exposure on derivatives and off-balance sheet contracts

A simple view of current exposure (the mark-to-market value owed by the counterparty) is not enough. Banks need to estimate Potential Future Exposure (PFE) – the possible increase in exposure over time due to market movements – especially for longer-tenor interest rate swaps or other volatile contracts. Historically, many mid-sized banks used the Current Exposure Method (CEM), a formulaic approach that adds a fixed buffer to current exposure. Now, best practice (and regulatory direction via SA-CCR) is to use more risk-sensitive methods, factoring in volatilities and correlations. Measuring PFE, expected exposure (EE) and related metrics is crucial to quantify how big a loss could occur if a counterparty defaulted in the future when the trade is in loss to the bank.

Robust limit setting and monitoring

Mid-sized banks typically set counterparty credit limits for loan exposures, but they may not have integrated derivatives exposure into the same limit framework. They need an enterprise-wide view of each counterparty's total exposure (loans + derivatives + other credit extensions) and to set limits that reflect the counterparty's risk. Moreover, these limits must be monitored continuously.

Modern CCR systems provide real-time limit monitoring and alerts. For example, if a customer's interest rate swap position starts generating a large exposure (such as if rates move and the customer owes the bank $50 million, approaching the credit limit), the system should flag this and potentially prevent new trades (pre-trade checks) until exposure comes down or the limit is increased after review. Many mid-tier banks currently lack such real-time, automated limit control – a gap that regulators will expect them to close.

Credit mitigation through collateral and netting

Robust collateral agreements (CSAs for derivatives) and netting arrangements are essential to mitigating CCR. Big banks typically require daily margin (variation margin) on swaps from financial counterparties and even from larger commercial clients to cover mark-to-market exposure. Mid-sized banks have sometimes been more lax, perhaps doing unsecured swaps with certain clients or only calling collateral infrequently.

But the recent guidance and sound practices emphasize that banks should actively use margining to mitigate counterparty risk wherever feasible. This means mid-sized banks need the operational capacity to handle daily margin calls, track collateral and enforce thresholds. Integrating collateral management into CCR systems is vital – the bank's risk calculations should consider collateral posted so that exposure is net of it – and also anticipate when more collateral will be needed.

Additionally, netting agreements (ISDA Master Agreements) that allow offsetting multiple trades with a counterparty are key to reducing effective exposure. Regulators will expect even mid-sized banks to have industry-standard documentation and to model the risk reduction from netting and collateral properly in their exposure metrics.

Stress testing and "what-if" analysis

Supervisors have highlighted the need for banks to stress test their CCR exposures under adverse scenarios. For example, what if interest rates spike by 300 bps and a hedging client can't meet a margin call? Or if a major counterparty – say a large broker-dealer – defaults during a market downturn?

Mid-sized banks historically have performed stress tests primarily for loan credit risk and interest rate risk in the banking book. Now they are expected to incorporate counterparty defaults and market shocks affecting derivatives into their stress frameworks. This requires more advanced analytics – simulating joint movements of market prices and counterparty credit events (including wrong-way risk, where exposure to a counterparty rises just as that counterparty's condition deteriorates).

Many regional banks are in the early stages of developing such CCR stress tests. They will need to invest in tools and expertise to perform them and then integrate the results into risk appetite decisions, e.g., setting capital buffers or limits based on stress outcomes.

Data aggregation and reporting

A fundamental but unglamorous need is good data infrastructure to aggregate CCR data across the bank. Mid-sized banks often have disparate systems – one system for loans, another for treasury/derivatives, and spreadsheets for certain exposures. This makes it hard to get a single number for "exposure to Counterparty X" or to produce timely reports for management and regulators.

But the new risk management expectations (like the Fed's guidance and Basel principles) stress accurate, timely reporting of risk. Mid-sized banks must be able to report, for instance, their top 10 counterparty exposures, or the magnitude of uncollateralized derivative exposure, or how much counterparty exposure would increase in a stress scenario.

Achieving this requires consolidating data onto a unified platform or warehouse, cleaning the data (e.g., ensuring legal entities are linked to the right parent counterparty), and automating report generation. It also means establishing watch lists and escalation processes. For example, if a particular counterparty is showing financial stress, the bank's CCR reports should flag that exposure for management attention – and possibly prompt actions like reducing positions or asking for more collateral.

Experienced risk personnel and governance

Lastly, a less quantifiable but still critical need is having the right people and processes to manage CCR. This means credit analysts who understand complex counterparty risk, including non-bank financial institutions; risk managers who can set prudent policies, like when to demand collateral or when to scale back exposures; and governance committees to review large exposures or exceptions.

For some mid-size banks, this is a cultural shift – moving from relationship-driven approaches ("Trust the long-time client") to more formal, analytically driven risk oversight. The new FDIC guidelines would even require banks >$50B to have a board-level Risk Committee, chaired by an independent director, to regularly review risk reports, including CCR metrics. Therefore, mid-sized banks need to cultivate expertise in counterparty risk and ensure their governance structures give CCR due attention – for example by including derivatives exposures in their credit risk appetite, not just loans.

These needs are underscored by recent events. For instance, the $10 billion loss across banks from the Archegos Capital Management default in 2021 – while affecting mostly large banks – served as a warning that poor counterparty diligence and slow reaction to mounting exposures can be disastrous. Closer to home, some regional banks got caught in energy price swings or rapid interest rate moves that strained their counterparties.

As the Basel Committee noted in April 2024, fundamental CCR practices at many banks remain inadequate, and improvements are "particularly urgent" for banks with concentrated or complex counterparty exposures.

The takeaway: Mid-sized banks may not deal with as many hedge funds or commodities traders as bulge-bracket banks do, but they still face significant CCR from activities like municipal derivatives, interest rate hedges and interbank placements. With their generally smaller capital base, a single counterparty default can have an outsized impact if not managed prudently. Hence, the call to action is clear: these banks need to shore up their counterparty risk defenses.

Building robust CCR systems: Requirements and solutions

To meet the challenges outlined above, mid-sized banks will need to implement robust CCR systems and frameworks.

A "robust" CCR system goes beyond basic credit tracking – it provides an integrated, real-time and predictive view of counterparty risk, and it supports the bank's risk managers in controlling that risk. Below we outline the key requirements for such a system and how modern technology solutions – often cloud-enabled – can fulfill them. We also compare how these capabilities improve upon traditional approaches.

CCR management aspect	Old approach (gaps)	Enhanced approach (requirements)
Exposure measurement	Simplistic exposure metrics (notional or current value) and static add-ons. Often uses the outdated CEM formula for derivatives.	**Risk-sensitive exposure analytics:** Calculate Potential Future Exposure (PFE), Expected Exposure (EE) profiles, and Credit Valuation Adjustment (CVA) using simulation or standardized methods. Reflect netting and collateral in exposures. E.g., implement SA-CCR for more accurate derivative exposure calculation.
Risk monitoring and limits	Siloed systems for different products; infrequent and manual limit checking. Limited ability to aggregate exposures across trading and lending.	**Enterprise-wide limit management:** Real-time consolidation of all exposures to a counterparty (loans + derivatives + repo, etc.) and automated limits monitoring with alerts. Perform pre-trade credit checks – new trades are instantly evaluated against available credit lines, preventing inadvertent limit breaches.
Collateral and margining	Collateral calls weekly or not at all for many clients; reliance on unsecured thresholds. Manual tracking of collateral.	**Active collateral management:** Daily variation margin and periodic initial margin as needed, managed through system that tracks collateral balances and requirements. Optimize netting and CSA terms – the system should evaluate exposure reduction from netting sets and collateral agreements, and forecast when margin calls will be needed. Integration of collateral data ensures exposures are calculated net of collateral held.
Stress testing and scenarios	Annual or ad-hoc stress tests that focus on loan portfolio; derivative exposures not stress-tested in an integrated way.	**Comprehensive CCR stress testing:** Incorporate market shock scenarios (interest rate swings, credit spread jumps, commodity price crashes) and counterparty defaults. Identify wrong-way risk – where exposure to a counterparty increases as that counterparty's health deteriorates – and model it explicitly. Use scenario analysis tools to see impacts on exposure and capital if key counterparties fail, and feed results into contingency plans.
Data aggregation and reporting	Fragmented data across spreadsheets and disparate systems; risk reports produced with lag – possibly weeks after quarter-end.	**Integrated data and real-time reporting:** A single source of truth for all counterparty exposures, enabling on-demand reporting. Interactive dashboards with drill-down to trade-level detail. Regular reports to management/board showing top exposures, limit utilizations, and PFE distributions. Automated regulatory reports (Call Report CCR schedule, etc.) to ensure compliance.
Governance and workflow	Informal credit processes; approvals via emails. CCR not always separated from loan credit process.	**Structured CCR workflow:** Clear processes for counterparty onboarding (credit due diligence, legal entity checks), limit setting (with credit committee approval), and exception handling (e.g. if a limit breach is imminent or a counterparty's condition worsens, escalate to senior management). A dedicated team or unit oversees counterparty risk and reports to the CRO and Risk Committee regularly. Workflow tools can enforce that, for example, any increase in exposure beyond a threshold triggers a formal review and sign-off.

As shown above, a robust CCR system has many moving parts – from analytics to data management to processes. Implementing this may sound daunting for mid-sized banks, but modern technology solutions can simplify the journey. Increasingly, vendors offer integrated risk management software tailored for banks of different sizes that encompass these features out-of-the-box. Such systems are often cloud-enabled, which drastically reduces the infrastructure burden on the bank.

A critical aspect of these modern solutions is their ability to handle large computation loads efficiently. Counterparty risk calculations – especially running simulations for PFE or doing full revaluation of a derivative portfolio under stress – can be computationally intensive. In fact, it's estimated that a mid-sized bank's derivative portfolio analysis might involve over 25 trillion trade valuations when doing complex exposure simulations. This is where technology shines: advanced CCR engines use optimized algorithms and parallel processing to crunch numbers quickly, and cloud platforms allow scaling up CPU/GPU power on demand.

For example, one of the largest bank's CCR and XVA engine increased calculation speeds by 10x and enabled on-demand intra-day risk calculations that were previously infeasible. While this bank is a global giant, the underlying concept applies to smaller banks too – by leveraging cloud computing, even a mid-tier bank can run sophisticated risk models (like Monte Carlo simulations) for PFE or full revaluation stress tests in a reasonable time frame without an enormous investment in hardware.

Robust CCR management also requires strong integration with other risk areas. Market risk and liquidity risk intersect with CCR – e.g., if a counterparty fails, the bank may have to replace trades in the market (market risk) and may need liquidity to post as collateral elsewhere (liquidity risk).

Modern systems therefore often integrate market risk metrics such as Value-at-Risk and have modules for funding valuation adjustments. They also tie into core banking systems to pull loan exposures, since a true single counterparty view needs both loan and derivative exposures aggregated. Other features might include flexible data integration (to link various data sources), scalability to growing volumes, and real-time analytics as key considerations. Additionally, compliance features, such as support for regulations like the upcoming Fundamental Review of the Trading Book (FRTB) for market risk and Basel III capital rules for CCR, are built-in so that reporting those metrics is straightforward.

Of course, technology alone isn't a panacea – banks must also update their internal policies and train staff to effectively use these systems. For instance, having a fancy PFE model is useless if the bank's credit team doesn't understand its results or fails to act on early warnings. Therefore, along with system implementation, banks are investing in talent and training: sending risk staff for training on derivatives, hiring quantitative analysts who can validate exposure models, and rehearsing default management drills (e.g., "What do we do if a counterparty suddenly can't pay?").

In addition, regulators will likely evaluate not just the presence of systems, but how the bank uses them. Does the board see CCR metrics? Do business lines have incentives aligned with CCR limits (not just revenue)? These governance enhancements complement the technical toolkit.

The takeaway: Mid-sized banks can – and must – achieve a step-change in CCR management by adopting integrated systems that provide a single view of risk, enforcing disciplined risk processes, and leveraging modern computing to run advanced risk analytics.

The good news is that technology has advanced to make this feasible and scalable, even outside the top-tier banks. In the next section, we delve into one of the most important enablers of this transformation: cloud-based and secure technology solutions that offer mid-sized institutions a fast track to world-class risk management capabilities without breaking the bank.

Embracing cloud-based, secure CCR technology

Cloud computing has become a game-changer for mid-sized banks that are upgrading their risk systems, including CCR management.

Traditionally, sophisticated risk analytics were the domain of only the largest banks, as they could afford vast on-premise hardware and software deployments. Today, however, forward looking vendors, such as Amazon Web Services, are delivering powerful CCR solutions via cloud platforms.

This shift offers several important benefits:

Scalability and performance

Cloud infrastructure provides virtually unlimited computing power on demand. Banks can run intensive calculations when needed and pay for only what they use. This elasticity is crucial for CCR, where workloads can spike during stress tests or when adding many new trades.

For example, the large global bank moved its counterparty risk and XVA engine to Google Cloud and achieved a tenfold increase in calculation speed. They can now perform full revaluations and sensitivity analyses intra-day, whereas before these might be overnight or not possible.

A mid-sized bank using a cloud-based risk solution might not need to increase their calculation speed tenfold, but even a 2-3x speedup can enable, say, daily PFE calculations instead of monthly, or the ability to run 1000 scenario simulations where only 100 were run before.

Using the cloud also enables systems to handle growth – if the bank's portfolio doubles or if regulators impose more complex metrics, the bank can scale up processing in the cloud instead of implementing a painful hardware procurement and upgrade cycle.

Lower cost and maintenance burden

Maintaining high-performance risk infrastructure in-house is expensive – servers, cooling, software licenses – and requires specialized IT staff. Cloud-based risk solutions often come as Software-as-a-Service (SaaS), where the vendor manages the software and hardware environment, and the bank just accesses it via secure connections. This dramatically lowers upfront costs and ongoing maintenance. Thus, mid-sized banks can implement robust CCR systems without building a mini data center. Additionally, updates for new regulatory changes or product enhancements are often handled by the provider and rolled out seamlessly, reducing the burden on the bank's IT teams to implement upgrades.

Rapid deployment and innovation

Cloud-based systems can be deployed faster than traditional on-prem software. There is no need to procure and install physical machines; instead, environments can be spun up in minutes.

Cloud also facilitates innovation. Banks can test new models or analytics in isolated cloud sandboxes without disrupting their main system. If the tests are successful, such models and analytics can be integrated into production rapidly. This opens the door for mid-sized banks to use advanced techniques like machine learning for credit scoring or AI for anomaly detection in exposures, which they might not have tried in a constrained IT setting.

Secure and compliant environment

Early on, banks hesitated about the cloud due to data security concerns. Those concerns have largely been addressed. Today's cloud providers and risk SaaS vendors implement bank-grade security measures: data encryption at rest and in transit, strong identity and access management, network isolation, continuous monitoring and regular security audits. Many are certified for industry standards (ISO 27001, SOC 2, etc.) and compliant with regulations like GDPR for data protection.

Mid-sized banks, which are often regulated by the FDIC, OCC or Fed, must ensure that their cloud vendor(s) can satisfy FFIEC guidance on outsourcing and cloud security – and many vendors have built-in compliance with U.S. banking security guidelines.

Data residency is another consideration: banks can choose cloud data centers in U.S. regions to address any locality requirements. Importantly, banks maintain control over their data – the contract will typically specify that the bank owns the data and the vendor cannot use it except to operate the service.

Disaster recovery and reliability

Cloud solutions inherently offer robust disaster recovery, as data can be replicated across multiple regions. A mid-sized bank using a cloud-based CCR system benefits from the provider's high availability architecture – if one data center goes down, another can take over, often transparently. This level of continuity might be hard for a smaller institution to achieve on its own.

It also aids in business continuity planning. For instance, during a regional disruption like a natural disaster, bank staff can access the cloud system from anywhere to monitor and manage risks, since it's not tied to a physical server in a branch. The events of 2020 proved the value of such flexibility, when lockdowns forced risk teams to work from home but still keep an eye on markets and counterparties using remote access to systems.

Of course, moving to the cloud comes with responsibilities: banks must perform due diligence on vendors, establish strong third-party risk management oversight, and have contingency plans (e.g., what if the cloud provider has an outage). Regulators will ask mid-sized banks for their cloud risk assessments and incident response plans. But these are manageable with proper planning and today are standard practice. Indeed, regulators themselves increasingly use cloud services for their data analytics, indicating their own confidence in the technology when properly secured.

Security features of cloud-based CCR solutions typically include end-to-end encryption, role-based access controls (so only authorized personnel can view sensitive counterparty data), multi-factor authentication for users, extensive logging of user activity (important for audits), and network security controls like firewalls and virtual private clouds. Additionally, many systems support data anonymization or masking in non-production environments, so if the bank is testing or if analytics are done on shared infrastructure, actual customer identities aren't exposed.

These controls give confidence that using the cloud doesn't mean compromising confidentiality or integrity of the bank's data. In many cases, a well-run cloud environment can be more secure than a patchwork in-house system, because dedicated security teams and advanced tools are guarding it.

The takeaway: Cloud-based CCR technology offers mid-sized banks a powerful combination of capability and practicality: they get cutting-edge risk analytics and system reliability that would rival a large bank's, delivered in a way that is cost-efficient and secure.

A concrete example of cloud technology benefiting CCR is in the computation of valuation adjustments (XVA). Calculating credit valuation adjustment (CVA) or debit valuation adjustment (DVA) involves simulating random paths of market risk factors and counterparty defaults – essentially combining Monte Carlo simulation with credit modeling, which is computationally heavy.

Once, a mid-sized bank might have skipped doing XVA due to its complexity. Now, with cloud power, they can run these calculations, or a vendor can offer XVA as part of the service.

In the case of the large global bank, their cloud risk engine covers CCR and XVA together, allowing integrated management of pricing and risk. Mid-sized banks can similarly start to incorporate CVA into pricing for customer trades, ensuring they charge appropriately for counterparty risk, once they have the tools to calculate it accurately.

Cloud advantages

- **Elastic computing:** Scale risk calculations on-demand (e.g., run 10,000 simulations fast).
- **Lower IT overhead:** Vendors manage updates and hardware, freeing bank resources
- **Fast deployment**: Launch new risk apps in weeks, not months.

Security by design

Modern cloud risk platforms embed encryption, rigorous access control, and 24/7 monitoring. Banks like the large global bank enforced stringent data standards and got regulatory greenlight for cloud risk engines. Vendors comply with bank regs (SOC 2, etc.), ensuring a secure environment.

The focus then shifts to how well the bank uses it, rather than whether they can build it. Many mid-sized banks are already taking this route, either by onboarding vendor SaaS platforms or migrating components of their risk infrastructure to the cloud. This trend is expected to continue, especially as banks confront tight deadlines to implement new capital rules or stress tests where buying a cloud solution is far quicker than building in-house.

Looking ahead, cloud adoption also opens the door for advanced analytics and innovation in CCR. With virtually unlimited compute and storage, banks can harness technologies like machine learning to identify patterns in counterparty behavior, such as early warning signs from trading patterns or news sentiment, or run complex climate risk scenarios that involve hundreds of variables.

In fact, one large global bank noted that with their new cloud-based framework, they can readily examine scenarios such as the impact of climate change on their portfolios – something that would have been very cumbersome before.

Mid-sized banks may eventually use these capabilities for internal risk insight – for example, analyzing how a rapid transition to a low-carbon economy might affect the default risk of their energy sector counterparties. Thus, embracing the cloud is not just about meeting today's needs but also ready-proofing CCR management for emerging risks and analytics techniques.

Future outlook and recommendations

The convergence of regulatory pressure and technological opportunity puts mid-sized U.S. banks at a crossroads for CCR management. Over the next five years, we expect:

Full implementation of new rules
By 2028, assuming current proposals are finalized, banks in the $50–$100B range will be fully subject to enhanced capital requirements, including holding capital for CVA and using SA-CCR for all derivatives.

Banks in the $10–$50B range will have had to comply with the FDIC's heightened risk management standards well before then – likely by late-2025–2026. This means the time to act is now.

Regulators have signaled that even before rules are final, their supervisors' expectations in exams are rising. Demonstrating proactive improvements could also stave off harsher measures.

Elevated role of risk management in mid-sized banks
We will likely see a cultural shift, where risk management, including CCR, gains a stronger voice in mid-sized institutions. Board members are paying closer attention to risk reports. It's expected that Board Risk Committees and senior management will routinely discuss counterparty exposures as part of strategic decisions, such as setting limits on how much derivatives activity to undertake with any single counterparty or sector.

In some cases, mid-sized banks might scale back or more tightly control certain higher-risk activities. For example, if a regional bank is dabbling in capital markets transactions with thinly capitalized non-bank entities, it may re-evaluate the risk/reward in light of Archegos-type scenarios.

Conversely, banks strong in risk management might capitalize on it, marketing themselves as safe derivatives partners to clients and potentially absorbing business from weaker competitors.

Incorporation of ESG and climate considerations

As sustainability continues to be a priority, even CCR management will incorporate climate and ESG factors. Regulators such as the Fed and OCC have started climate risk pilots for large banks, and over the next few years they may roll out climate risk management expectations to smaller banks. This could involve assessing how environmental factors affect counterparty creditworthiness.

For instance, a mid-sized bank might need to evaluate the carbon transition risk of its counterparties – e.g., if it provides commodity hedges to an oil and gas firm, what is the long-term default risk of that firm under various climate policy scenarios?

In CCR terms, this might mean including climate stress scenarios in counterparty stress testing, such as a scenario where carbon prices soar and an oil counterparty's financials deteriorate. Additionally, qualitative ESG factors might be included in counterparty due diligence – for example, poor governance or transparency (a "G" issue) might warrant more conservative risk limits.

While this is still nascent, banks that build flexible CCR systems now will be better able to integrate such factors. The HSBC cloud risk platform example, where they can simulate climate impacts and adapt quickly, is a bellwether.

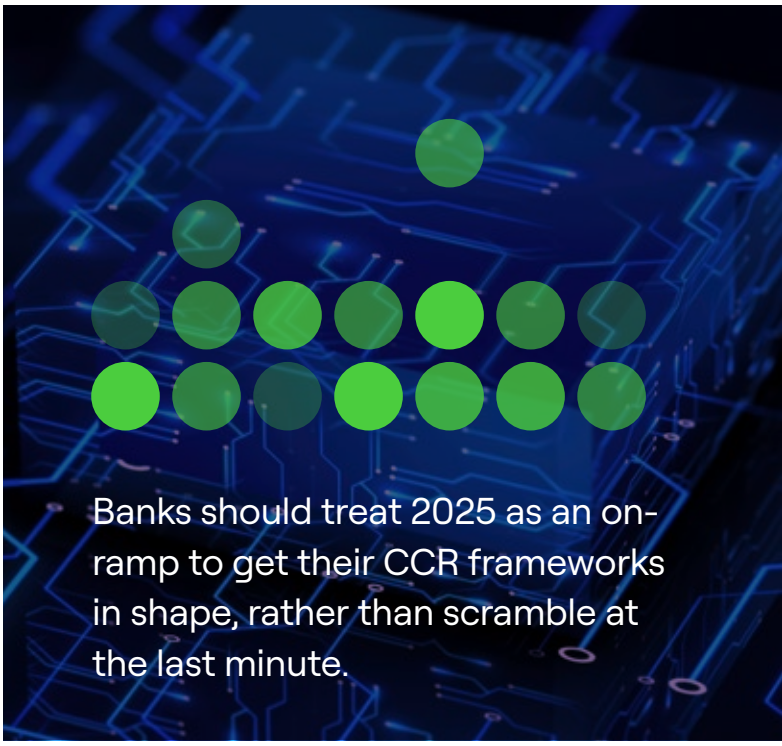
Greater interconnectedness monitoring

Recent market events, such as the U.K.'s LDI pension fund near-meltdown in 2022, which had ripple effects globally, have taught regulators that mid-sized banks cannot ignore indirect risk from the broader system. Expect more focus on concentration risk and correlation in CCR. Banks will be encouraged (or required) to monitor concentrations to certain sectors or types of counterparties. For example, a regional bank might discover that many of its derivative exposures are to energy trading firms – a concentration that could be risky if that sector hits turbulence.

Also, banks should be aware of how their counterparties are interconnected – if several counterparties are all exposed to the same stress, the bank faces a cluster of potential defaults. Regulators like the Basel Committee emphasize understanding correlations and wrong-way risk in CCR. We anticipate that mid-sized banks will adopt tools to map these interconnections, perhaps using network analysis or enhanced reporting, so they can avoid unseen pockets of risk.

Industry collaboration and utilities

Managing CCR, especially aspects like counterparty data and analytics, could spur more collaboration among mid-sized banks. Just as large banks created utility companies for things like KYC data sharing, regionals might band together for risk management utilities. For example, a consortium of banks could share a cloud-based database of counterparty financial statements or credit scores, or they could jointly invest in a platform for scenario analysis tailored to mid-sized institutions. This could help spread cost and share best practices.



Another area is central clearing: regulators might encourage more use of central counterparties (CCPs) for derivative trades to reduce bilateral exposures. If clearing access becomes easier for smaller banks (possibly through intermediaries), then within five years we could see a larger portion of regional banks' derivatives centrally cleared, which mitigates CCR (shifting it to CCP default risk, which is separately managed via the CCP).

Potential consolidation

As noted by industry analysts, the rising compliance and capital costs could drive consolidation in the regional bank sector. If some banks find the new requirements too burdensome or capital-dilutive, they might seek mergers. Banks that have invested in robust risk management will be more attractive partners (and more likely to be survivors). In a consolidation scenario, having a strong CCR infrastructure is an asset – it eases the due diligence process, and the merged entity can build on it.

Conversely, banks with weak risk controls might struggle to find a dance partner or could be acquired at a discount. Thus, making these improvements is not just about compliance; it could determine strategic outcomes.

5 recommendations for mid-sized banks:

1. Accelerate CCR system projects

Don't wait for final rules – begin upgrading counterparty risk systems now. Consider cloud-based solutions that can be implemented in phases, focusing first on high-priority needs, such as exposure aggregation and limit management, and later extending to advanced modeling. Quick wins like getting a consolidated exposure report or setting up automated limit alerts can materially improve risk control in the interim.

2. Strengthen counterparty due diligence

Review and enhance counterparty onboarding processes as per emerging guidelines. When taking on a new derivatives client or counterparty, conduct thorough credit analysis, including qualitative factors. Periodically refresh this analysis – don't adopt a "set and forget" mentality. Establish criteria for when a counterparty must provide financial disclosures or collateral; smaller banks sometimes transact based on long relationships, which must be complemented with formal credit evaluation.

3. Integrate CCR into an enterprise risk framework

Counterparty risk should be part of the enterprise risk appetite statement and included in risk reporting that goes to the CEO and board. For example, if the bank has a risk appetite metric like "Top 10 counterparty exposures not to exceed X% of capital," then track and report that regularly. Align the treasury, lending and risk teams so that a large loan to a company and a swap with the same company are viewed together, not separately. Break down any silos between the loan credit team and the capital markets team – perhaps create a joint Credit & Counterparty Risk Committee to discuss overlaps.

4. Prepare for regulatory interactions

As examiners intensify their scrutiny, be ready to demonstrate progress. Document your CCR enhancements, have clear narratives for your risk model choices – such as how you calculate PFE and why it's sufficient for your portfolio – and perform internal audits or validations of your CCR processes. Regulators will likely ask mid-sized banks for self-assessments against new guidelines, so it could be wise to conduct a gap analysis now (and many firms engage consultants to do this for them). Identify and address gaps in people, process or technology. If certain things can't be fixed immediately, have a roadmap that you can show regulators, indicating commitments to improvement.

5. Leverage external expertise and training

Utilize industry groups like the RMA and PRMIA, as well as consultants, to share best practices on CCR for mid-sized institutions. Regulators have hinted at common weaknesses like fragmented systems and insufficient stress tests – learn how peers are tackling these.

Train your risk and front-office teams on new models (for example, how SA-CCR works, since that will drive capital numbers). Bridging the knowledge gap is key; if front-line businesspeople understand that, say, uncollateralized swaps now consume significantly more capital under SA-CCR, they can price and negotiate those deals differently – or decide not to do them. Essentially, create a strong risk culture where counterparty risk is everyone's business, not just the responsibility of the risk department.

The takeaway: Mid-sized U.S. banks must evolve their CCR management from basic to cutting-edge. Regulatory drivers make it non-negotiable, but beyond compliance, it's simply sound business in a volatile world. The tools and technology are more accessible than ever – cloud solutions and advanced analytics can be the great equalizer, allowing a $30B bank to manage complex risks nearly as well as a $300B bank.

The coming years will likely separate the leaders from laggards in the regional banking segment based on risk management prowess. Those that invest early in robust CCR frameworks will not only satisfy their regulators but also enjoy greater confidence from counterparties, rating agencies and investors. They will be more resilient in the face of shocks – whether a sudden counterparty default or an extreme market event – and better positioned to seize opportunities (for instance, stepping in to serve clients left orphaned by less risk-equipped competitors).

Ultimately, strong CCR management is about safeguarding the bank's stability while enabling healthy growth. By understanding their exposures in depth, controlling them proactively, and utilizing secure, scalable technology, mid-sized banks can turn what could be a regulatory headache into a strategic advantage. The path forward involves prudent adaptation and embracing innovation – a combination that will define the next generation of regional banking success.

Summary

FIS® Enterprise Risk Suite helps financial institutions manage market and counterparty credit risk and make better risk management decisions. The solution allows you to consolidate, simplify and optimize your organization's risk infrastructure to help advance the way you manage risk and make capital work harder.

As regulations and market dynamics continue to evolve, risk managers must track a growing range of risks in ever greater detail. Now available in the cloud, Enterprise Risk Suite provides the advanced computational resources you need to handle this complexity, while helping reduce risk infrastructure costs and increase synergies across your risk management team.

Unlock Risk Management

Money at rest. Money in motion. Money at work.™

FIS risk management solutions help you work your capital harder. Our technology powers the global economy across the money lifecycle.

Money at rest

Unlock seamless integration and human-centric digital experiences while ensuring efficiency, stability, and compliance as your business grows.

Money in motion

Unlock liquidity and flow of funds by synchronizing transactions, payment systems, and financial networks without compromising speed or security.

Money at work

Unlock a cohesive financial ecosystem and insights for strategic decisions to expand operations while optimizing performance.

fisglobal.com/contact-us linkedin.com/company/fis x.com/fisglobal

FIS | Advancing the way the world pays, banks and invests™