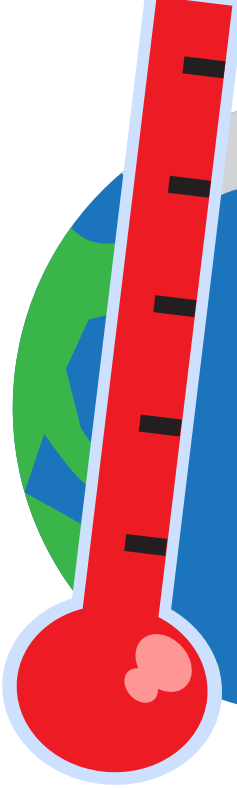
PERSPECTIVES

BANK RISK MANAGEMENT IN THE AGE OF DISRUPTION:

AN ACTION PLAN FOR BOARD DIRECTORS AND CHIEF RISK OFFICERS



By James C. Lam

We are living in disruptive times. Enterprise value is being destroyed (and created) at an unprecedented speed. A recent McKinsey study found the average time a company is listed in the S&P 500 has dropped from 61 years in 1958 to less than 18 years today. McKinsey estimates that 75% of S&P 500 companies today will disappear from the index by 2027.

A major source of this disruption is the confluence of traditional and emerging risks. Traditional risks are often defined as strategic, operational, financial, legal/regulatory, and reputational risks. Emerging risks vary by industry, but many surveys cite geopolitical instability and conflict, digital transformation (for example: AI, blockchain, and quantum computing), cybersecurity, climate change, and financial markets fragility.

The interaction between traditional and emerging risks can have unexpected and sudden impacts. We witnessed this last spring, when the modern phenomena of cryptocurrency-related deposits, social media chatter, and lightning-fast digital withdrawals—in combination with old-fashioned asset/liability management issues—prompted three bank failures over the course of five days.

In this environment, board risk oversight and ERM are more important than ever. But with growing complexities and challenges, banks can't afford to do more of the same. And the resources to keep adding more people, processes, and systems are limited. It makes sense,

then, to rationalize resources by eliminating conventional risk management tools that don't add value and invest in new practices that will lead to faster and better decisions. This article provides actionable ideas for board directors, CROs, and other bank leaders to rationalize their risk management resources and simultaneously manage traditional and emerging risks.

Heightened Regulatory and Disclosure Standards

While regulatory and disclosure risks are often viewed as traditional risks, they can be dynamic and challenging. Bank directors and executives often face new and heightened standards from regulators, investors, and other key stakeholders. That is shaping up to be the case again following last spring's liquidity crisis.

In detailing Silicon Valley Bank's failure, the Federal Reserve noted traditional risks—including a concentrated business model, uninsured deposits, and an asset/liability duration mismatch—and how the combination of social media, a networked depositor base, and digital banking dramatically increased the speed of the bank run. Going forward, banks should expect heightened regulatory and supervisory standards for asset/liability management, liquidity risk management, and capital and liquidity management, as well as requirements for stress-testing the bank's vulnerability to emerging technologies and risks.

In addition, public companies face new disclosure requirements for emerging risks that go beyond generic 10-K risk disclosures. For example, on July 26, 2023, the Securities and Exchange Commission adopted a final cybersecurity disclosure rule that requires public companies to disclose material information on their cybersecurity risk management, strategy, and governance. Companies are also required to report material cybersecurity incidents within four days, including financial and operational impact.

Lessons Learned From the Banking Failures

This year's banking failures offer important lessons for management and the board. Key takeaways for management include:

- Select a CRO with the right skills and empower that CRO with independence and authority. For example, the CRO should not only help set risk appetite limits but also be able to enforce them when actual risk exposures are too high.
- Analytical models and contingency plans must consider the confluence of traditional and emerging risks, including key interdependencies and specific scenarios. Risks are not static. Prepare for critical upside and downside scenarios that encompass multiple risks.
- An effective model risk governance and management framework must be in place. The scope of this framework should include traditional risk models (e.g., ALM) and emerging technologies (e.g., generative AI) and define appropriate use cases, prohibited use cases, and approval and reporting processes for model changes.

Key takeaways for the full board and each of its committees include:

- The full board is responsible for strategy, and as such, overseeing strategic risk. It should oversee reputational risk, and during a crisis, stakeholder communications.
- The risk committee should have an effective reporting relationship with the CRO and ensure that risk appetite tolerances are clearly defined and enforced.
- The audit committee should ensure that financial statements provide stakeholders with transparency on the bank's risk profile, including traditional and emerging risks.

- The governance committee should define risk oversight responsibilities for the board and its committees, as well as ensure that they have appropriate risk management expertise.
- The compensation committee should ensure that incentives do not encourage excessive risk-taking, and that CEO and executive reviews consider risk-adjusted performance.

Common Pitfalls To Avoid

When faced with a combination of traditional and emerging risks, banks are ill-prepared if they are supported by inadequate risk management processes. As a CRO, consultant, and board director, I have worked on over 100 ERM programs across banking and other industries. Importantly, I have observed some common pitfalls in ERM and board risk oversight. I encourage board directors and CROs to: identify these pitfalls at their banks, discourage such conventional "check the box" practices, and reallocate valuable time and resources to the more useful processes outlined in the next section.

The following three "golden rules" encapsulate the major pitfalls to avoid:

Don't Do Stupid

I have seen risk teams use rudimentary risk control self-assessments (RCSAs) and heat maps to identify and report key risks to management and the board. The common methodology is to rate each risk from 1 to 5 (lowest to highest) for probability and severity. The probability rating is then multiplied by the severity rating to produce a "risk score," and the results are displayed on a heat map. Nonsensical results can be produced. For example, the risk score for a cyberattack that is blocked could be a 5 (or 5 times 1), given its inherent high probability (5) multiplied by its low severity (1). Yet the risk score for a cyberattack that results in a major data breach could also be a 5 (or 1 times 5), given its inherent low probability (1) and high severity (5). Better risk assessment methodologies reflect the fact that each risk has a range of probabilities and severities (i.e., a distribution curve) and that the variability of outcomes matters; they move beyond simple expected loss (probability times severity) because risk is much more about the difference between actual and expected losses (unexpected loss).

Don't Do Lazy

Risks are often defined and measured as nonperformance of a business objective. This is too simplistic. For example, if the company wants to maintain 99% or greater availability of its core operating systems, then the risk could be defined as downtime and measured against the 1% maximum allowance. That represents lazy thinking and produces backward-looking metrics and reports. Instead, risks should be defined as the underlying variables that can result in downtime. In this example, these underlying variables may be internal (IT capacity) and controllable (cybersecurity tools), as well as external (customer order flows) and uncontrollable (denial-of-service attacks). With better definition and quantification, more actionable metrics and useful reports can be produced.

"Risks are often defined and measured as nonperformance of a business objective. This is too simplistic."

Don't Do Boring

Board-level risk reports and presentations provided by risk, compliance, cybersecurity, and internal audit teams often focus on key accomplishments, progress reports, and major plans and initiatives. While well-intentioned, this information does not fully support the risk oversight role of the board. A concise summary or progress report is fine, but board directors are more interested in what risks and scenarios can impact the bank's strategy, earnings, and long-term value. The role of the board in risk oversight can be better served with contextualized, quantitative, outside-in, forward-looking, and decision-oriented information.

In a dynamic risk environment, banks cannot afford to waste limited resources on activities that don't add business value.

Action Items for Consideration

This age of disruption is prompting board directors and CROs to proactively monitor the maturity and effectiveness of their ERM programs. The following are five key areas for consideration in that effort:

Align ERM to Strategy and Culture

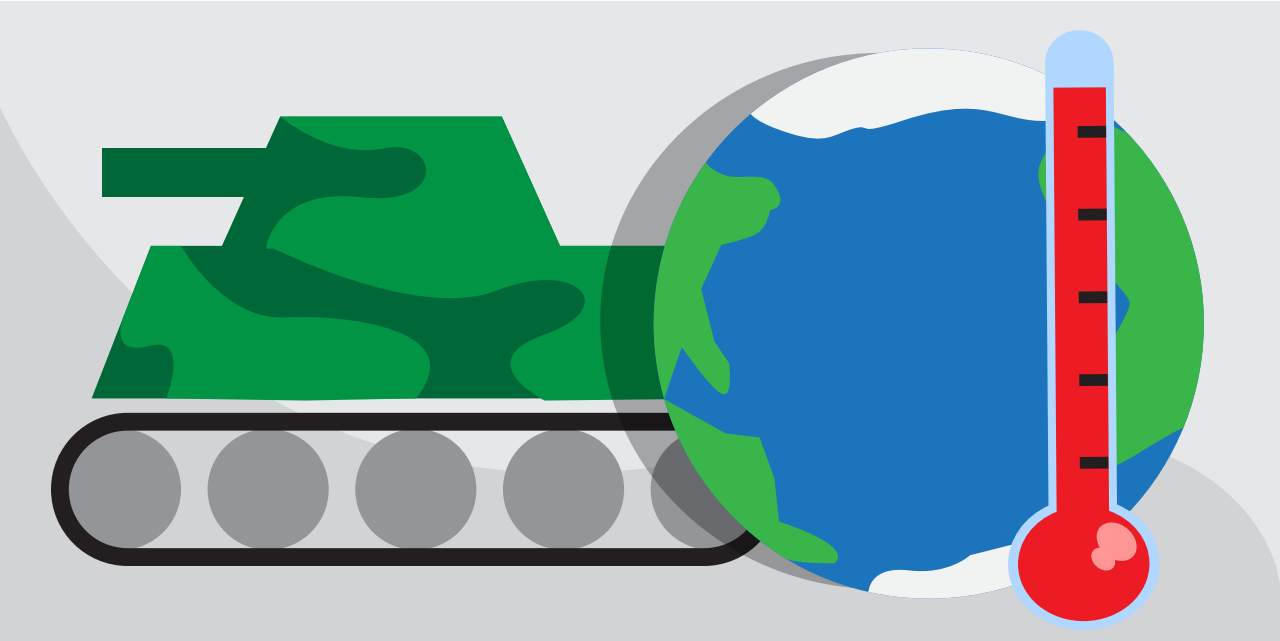
Numerous research studies have shown that strategic risks (e.g., M&A, new products, digital transformation) account for 60% of a company's risk profile, followed by operational risks (30%), and financial risks (10%). Given the importance of strategic risk, the board should oversee strategy and risk on an integrated basis. Fundamental steps include clearly defining strategic objectives; establishing key performance indicators (KPIs) to measure performance; assessing key traditional and emerging risks; establishing key risk indicators (KRIs) and risk appetite for these risks; and implementing integrated reporting and management processes. Peter Drucker famously said "culture eats strategy for breakfast" to argue that no matter how great a business strategy is, it will fail without the right people and culture to implement it. To enhance risk culture, banks can invest in ERM training programs, talent development initiatives, and risk culture surveys, and ensure that risk-adjusted performance incentives are in place to motivate the desired behavior.

Improve the Risk Appetite Statement and Application

The risk appetite statement (RAS) is one of the most important risk management policies. It defines, both in qualitative and quantitative terms, the risks that the bank is willing to accept. However, in a highly volatile and uncertain business environment, the RAS can no longer be a static document that is updated and approved by the board once a year. It needs to be dynamic and evolve with key considerations such as external risk drivers, internal risk capacity (e.g., capital, liquidity, and management skills), and risk/return trade-offs. The RAS should also be linked to two other essential board-level risk management policies: (a) the risk escalation policy that establishes thresholds for real-time communication of material risk events to senior management and the board, and (b) the risk acceptance policy that provides processes to approve and manage RAS policy exceptions.

Enhance Risk Reporting

The quality of risk reporting substantially influences the quality of management decisions and board risk oversight. The three common pitfalls discussed in the previous section often result in risk reports that are not useful to business leaders or board directors. A best-practice risk report would include an executive summary written by the CRO, external risk and regulatory trends, actual bank losses



and risk events, KRIs tracked against risk appetite tolerances for each risk area, and risk analytics such as economic capital and stress-testing. Effective risk reports are forward-looking and support decision making at the management and board levels.

Ensure Overall ERM Program Effectiveness

The key objective of ERM is to minimize unexpected performance variance. For example, on a monthly or quarterly basis, the bank can monitor unexpected earnings variance, which is calculated by comparing earnings-at-risk analysis at the beginning of the period with earnings-attribution analysis at the end of the period. Unexpected earnings variance should be within an acceptable level, say 20% of total earnings variance. Both traditional and emerging risks can increase unexpected earnings variance. The key is to identify, assess, and minimize such variances at an early stage.

Incorporate Emerging Risks in ERM

Banks face emerging risks such as geopolitical uncertainties, disruptive technologies, cybersecurity, and climate change. These emerging trends can create both new risks as well as new opportunities. For example, AI presents new challenges for job displacement, privacy concerns, ethical issues, security vulnerabilities, and data quality and bias. On the other hand, it can help banks improve customer service, create content, comply with KYC and AML regulations, monitor third-party vendor risk, and modernize data structures and models. A useful exercise is for directors and executives to form a working group, leverage scenario analysis techniques, and develop strategic plans for emerging risks. This is like table-top exercises for cybersecurity but focused on the disruptive risks facing the bank.

Banks are operating in the age of disruption. They must simultaneously manage traditional and emerging risks, as well as face heightened expectations from regulators, shareholders, and other key stakeholders. In this environment, it is imperative for bank directors and CROs to evaluate their board risk oversight and ERM practices, eliminate conventional processes that don't add value, and ensure that their risk governance, oversight, and management are fit for purpose.®

JAMES C. LAM is president of James Lam & Associates, a risk management consulting firm. He is a former board risk committee chair of E*TRADE Bank and former chief risk officer of Fidelity Investments. He is author of Enterprise Risk Management and Implementing Enterprise Risk Management, both published by Wiley. He can be reached at james@jameslam.com.