rma
THE RISK MANAGEMENT ASSOCIATION

JOIN. ENGAGE. LEAD.

OPERATIONAL RISK GOVERNANCE AND HEIGHTENED REGULATORY EXPECTATIONS:
5 CORE EXPECTATIONS

Enterprise Risk • Credit Risk • Market Risk • Operational Risk • Regulatory Compliance • Securities Lending

CONTENTS

HEIGHTENED EXPECTATIONS

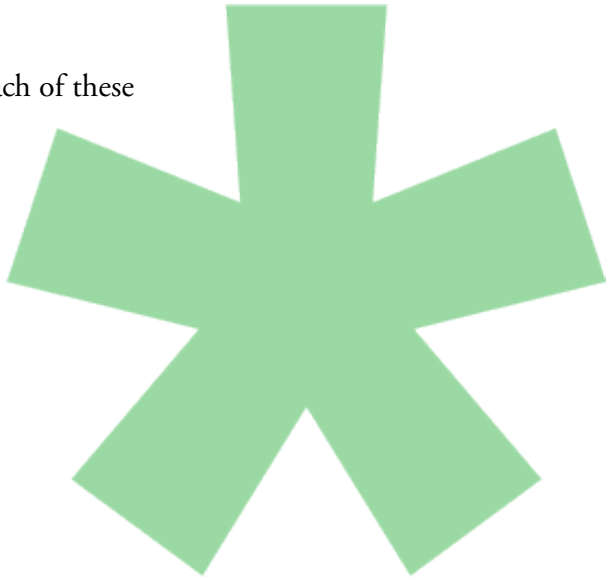
The concept of heightened expectations was no surprise to banks, even before the publication of the notice of proposed rulemaking (NPR) that appeared in the Federal Register on January 27, 2014 (Volume 79, No. 17, page 4282). The OCC had been raising these issues for years. The NPR however, did provide more detail on OCC expectations.

THE OCC's FIVE CORE EXPECTATIONS

1. The bank board must act in the best interests of the bank entity.
2. Banks must have well defined personnel management programs, including staffing, succession, and compensation programs that do not reward excessive risk taking.
3. Banks must articulate their risk appetite tolerance levels, using capital at risk, earnings at risk and liquidity measures. Limits should be established and allocated to lines of business.
4. Banks must have strong audit and risk management programs.
5. Bank boards must evidence their willingness to challenge and question bank management.

The proposed rule also includes considerable detail on expectations relating to first, second, and third lines of defense as part of the risk governance framework of the bank.

Operational risk governance alone will not meet each of these expectations, but it would difficult to comply fully without a solid governance framework.

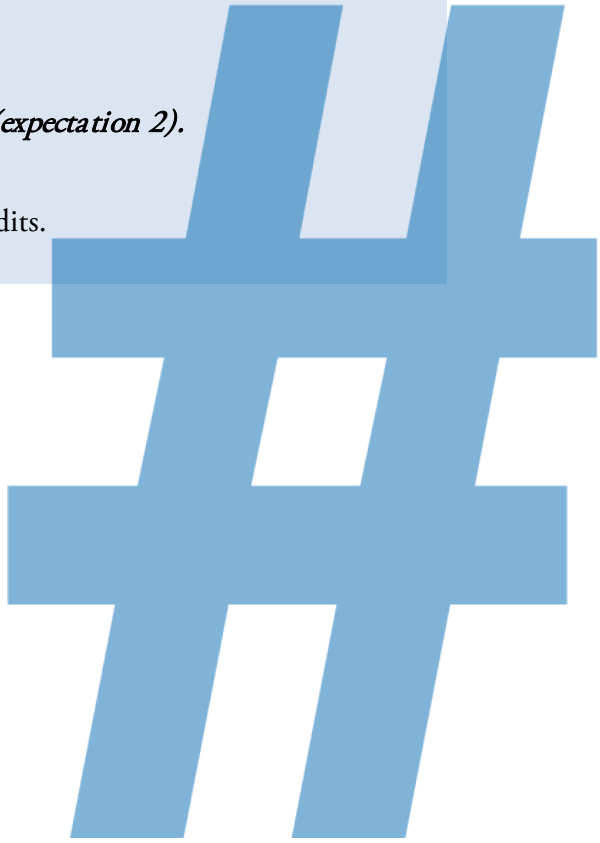


GOVERNANCE

In order to meet the expectation that the board will act in the best interests of the bank *(expectation 1)*, the board or the Risk Committee of the board must have accurate and relevant information about operational risks and any operational risk limits established under the comprehensive risk appetite framework. In the context of operational risk, such limits or measurements can include:

- Trading errors (dollars and count).
- Fraud losses (internal and external).
- Legal settlements.
- Control gaps.
- Measurement of self-identified issues vs. issues identified by second or third lines of defense.
- Regulatory violations.
- Severity and frequency of operational losses.
- Vendor errors or vendor concentration risk.
- System outages and recovery time.
- Information security breaches.
- Employee attrition and staffing adequacy *(expectation 2)*.
- Errors in new product launches.
- Failed branch, operations, and business audits.

3



GOVERNANCE ROUTINES

Management, especially executive management, should be well-aware of the operational risks affecting their business. Management must be accountable for their risk-taking activity.

- Management control assessments (similar to risk and control self assessments, but with more testing of controls) are a key tool to assess the level of operational risk.
- Key risk indicators should also be established and monitored for breaches or trend lines heading toward a KRI breach.
- An understanding of what drives increases or decreases in operational risk capital, or stress testing from operational risks (impact on EaR and VaR) is essential for strategic planning, the development of appropriate controls, and the allocation of IT and human resources *(expectation 3).*
- Information on all operational risks (emerging or extant) and associated metrics should be discussed in an operational risk committee meeting or should have a standing section in a comprehensive risk committee meeting in which all types of risks are discussed in one forum (preferred).

Change of any kind is a key operational risk, whether it is a merger, a sale or purchase of assets or liabilities, a new product launch, a systems conversion, a change in branch controls, or introducing a new product or service.

- A Change Control Committee, through which any proposed change to the control environment is brought for discussion and decision, is a valuable tool to prevent execution mistakes. The membership is generally comprised of business leaders, Risk Management, Technology, Operations, and Compliance.
- The Change Control Committee does not decide whether a proposal is appropriate in theory, or whether it poses a legal or regulatory risk that should have been vetted much earlier in other forums,
- The Change Control Committee's focus is to ensure that the teams have thought through everything that is needed to ensure an execution that is

consistent with expectations (i.e., no surprises). This includes the results of UAT or FUT, communications plans, checkpoints with key internal and external partners, and a plan for monitoring the change post-implementation.

- "Ready, aim, fire" is **always** better than "fire, ready, aim."

PERSONNEL AND ROLES/RESPONSIBILITIES

It is very important that the business understand the operational risks they are incurring.

It is also important that independent risk groups have personnel capable of developing operational risk policies, procedures, and programs consistent with the overall risk appetite framework of the bank. This requires risk managers with actual experience in transaction processing, technology, information security, and fraud detection and prevention ***(expectation 4).***

It is equally important that auditors have such experience.

THE BOARD

It is not only critical from a governance standpoint that the board be fully informed; it is also important that they be fully *engaged* ***(expectation 5).***

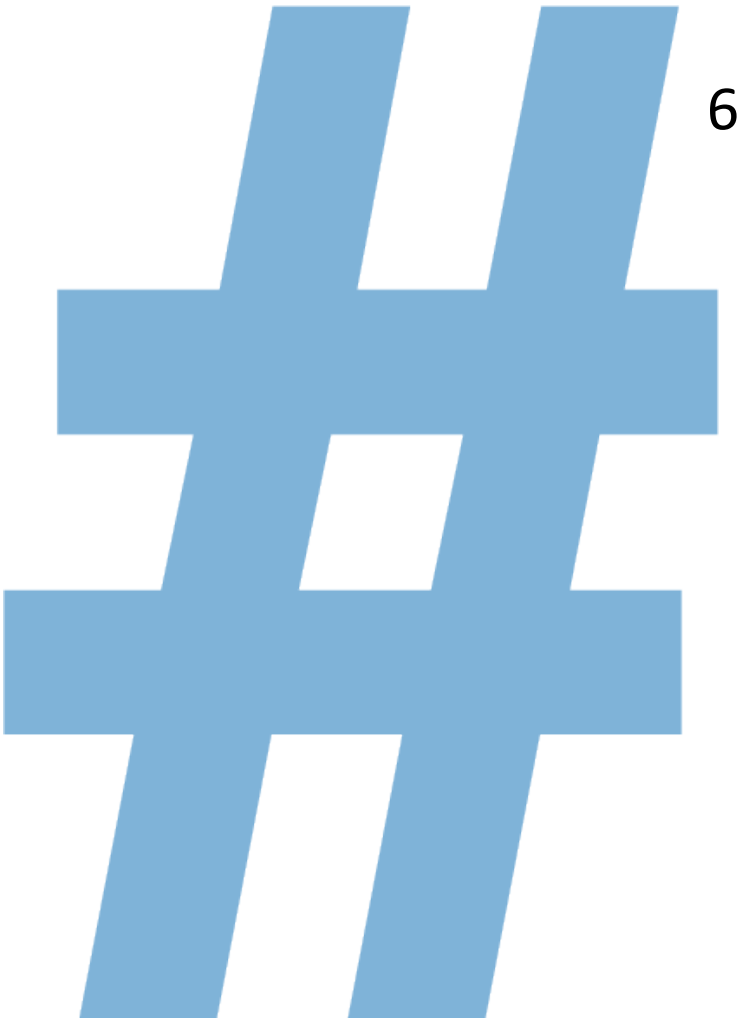
The board should have a healthy degree of skepticism. It doesn't mean they shouldn't trust management, but they should make sure they fully understand a situation. Key questions they might ask in the operational risk space might include:

- What was the root cause of that loss?
- How do you know it will not happen again?

EQUALLY IMPORTANT

Not only must the board be engaged, but you have to prove they are engaged. This means much more detailed minutes than may have been traditional, e.g., showing questions or challenges by the board directed to management and active discussion among the board members. Bank examiners cannot sign off on what they cannot see.

- What sort of testing of controls did you do to ensure that this gap is closed?
- So, you have closed this control gap….are there other similar gaps that need work? How do you know?
- How does this rank in terms of priority of risk focus? Why?
- Do you have the human and technology resources to address this issue?
- Who are our largest or key vendors?
- How confident are you that your vendor has their end under control? How do you know?
- I read about XYZ bank and the problem they had with XXX. Can this happen here? How do you know? What are you doing about it?



This whitepaper was adapted from a presentation given by Malcolm Griggs, Managing Director and Head of Risk and Controls at Citi, at RMA's 8th Annual Governance, Compliance, and Operational Risk Conference on May 7. Please save the date for GCOR IX, April 22–23, 2015 in Boston, MA

About RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues.

Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, these 16,000 individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

Phone: 800-677-7621
Fax: 215-446-4101
Website: www.rmahq.org

RMA University

In today's rapidly changing financial services industry, you need practical, day-to-day knowledge that will help you excel in your profession. RMA provides quality education to advance sound risk principles in the financial services industry. Traditional classroom training and online learning resources are available as open enrollments or in-bank training. Visit http://www.rmahq.org/events-training/rma-university/rma-university to learn more.

eStatement Studies

RMA's eStatement Studies℠ is the only source of comparative data that comes directly from the financial statements of small and medium-size business customers of RMA's member institutions. Round-the-clock online access gives you the ease and flexibility to use this wealth of information at your convenience. Visit http://www.rmahq.org/tools-publications/tools/estatement-studies to learn more.

Are you an RMA member?

An RMA membership provides many benefits. In addition to a free subscription to The RMA Journal® and discounts on RMA events, products, services, and training, membership also provides countless networking opportunities and exposure to the industry's key decision makers and manager. RMA's local and national events keep you up to date on industry trends and issues while allowing you to meet new people and swap successes with peers. Visit http://www.rmahq.org/joinrma to learn more about membership.