Operationalizing Risk Tolerance

Op·er·a·tion·al·ize
A made-up word
1. Its intended meaning here is what one might expect—the process of applying global principles to specific operational processes.

iStockphoto/Thinkstock

Never assume your risk tolerance strategy is being carried out properly just because it's been put down in words. To have real impact, it must be carefully aligned—or "operationalized"—throughout your organization.

BY ERIC HOLMQUIST

IT'S BECOMING COMMONPLACE for corporate risk management programs to set risk appetite and tolerance levels and to communicate them throughout the organization. Regulators are strongly encouraging the industry to adopt this practice.[1]

Such efforts make sense: Clearly defining and articulating acceptable risk levels is at the heart of what risk management really is, which is risk *alignment.* It's foundational to everything we do—and allow—in pursuit of return on investment.

Consider the rapid evolution of risk management over the past few decades. Twenty or 30 years ago, what we called "risk management" was really risk hedging, conducted largely through investment and insurance activities. The idea was to mitigate potentially life-ending events through one or more risk-transfer products. For the rest of the risks, it was manage-as-you-go.

Over time, risk management became more of a governance process that involved thinking more broadly about large events that could still be damaging—even catastrophic—but that could be mitigated through internal controls and risk monitoring. However, the focus was still largely on the "black swans": the large-impact, unexpected events. Today, the discipline emphasizes building awareness of risk at every level and continuously seeking opportunities to reduce it.

The risk management discipline is still not mature. Regardless of the number of assessments conducted, controls put in place, or reports generated, we can't escape the fundamental questions: "How much risk is enough?" and "What is the acceptable level?" We know risk is largely managed to an *assumed* level, and controls are almost always built to a perceived level of risk. If it feels risky, we create a control. If it still feels risky, we add another control. We continue until we have a consensus that the amount of controls is just about right.

But does the amount of risk the board and senior management expect to take equal the risk reflected in the aggregate of all internal processes, net of all risk treatment? The answer, sadly, is "We just don't know" or, in a best-case scenario, "We think so." That's a bitter pill for those who have been doing risk management for a while.

Establishing risk appetite and tolerance levels is not only critical, it is truly foundational—the basis on which *all* strategic decisions should be made. It is the standard that should be applied not only to strategic initiatives, but to all risk assessments. We should ask if our operations are aligned with our risk tolerance. When we can answer confidently, we will have reached an important and profound level of maturity in the risk management discipline.

This "operationalizing" aspect is truly important. Too often, and especially within the context of the recent financial crisis, senior management has tended to prioritize only those risks that could end the bank. We have to move out of this bunker mentality and start to look at our operations overall, because death by a thousand cuts can be just as damaging as long-tail events.

All businesses follow a common life cycle: 1) set strategy, 2) execute on it, and 3) periodically reassess to determine if a change of course is merited. Risk management needs to connect the dots between the point of strategy (where risk appetite is determined) and operations (how we implement that strategy). This is the key to enterprise risk management (ERM) and the piece that has been missing.

Tolerance statements should reflect the absolute boundaries beyond which the business simply will not go. These can be thought of as the perimeter fence to a cattle ranch.

To achieve the sought-after state of risk alignment, the organization needs an ERM model that can assess risk at strategic *and* operational levels because these are what we want to align. The risk profiles of the bank's operations, in aggregate, should reflect the same level of risk as the strategic view. If not, something has gone wrong in how risk appetite was communicated internally. It's as simple as that. An ERM framework that looks only at the big picture or at operations is looking at only one side of the equation, and it will be impossible to connect it all back to risk appetite, our foundation.

Definitions

People use terms differently, so it's important to have common definitions before getting into how we operationalize[2] risk appetite and risk tolerance values. For our purposes, the following definitions will apply:

- *Risk appetite:* General statements about the level of risk considered acceptable within a given risk category or type. These should serve as guiding principles when developing strategic plans, operational processes, and business continuity plans.
- *Risk tolerance:* Tangible risk limits designed to set specific boundaries in which the business must operate. These must be measurable, realistic, and capable of being monitored.

How an organization uses or defines its own similar terms is not important, so long as they are intuitive, universally understood, and consistently applied.

Establishing Risk Appetite and Tolerance

Senior management begins by establishing risk appetite and tolerance statements. These should consider broad business risks such as capital, growth, earnings, and corporate governance, as well as traditional risk categories such as credit, liquidity, interest rate, price/market, operational, reputation, compliance, and concentration. These represent two distinct perspectives or dimensions of risk.

While appetite statements can be general in nature, tolerance statements should reflect the absolute boundaries beyond which the business simply will not go. These can be thought of as the perimeter fence to a cattle ranch. Within these tolerance values the institution may also choose to identify additional intermediate values with associated management triggers. These values would likely be tied to key risk indicators that indicate to management when a key metric is heading in the wrong direction.

When establishing tolerance values, you must determine how they translate into operating rules at a process level. You will need to ask these questions:

- How will I measure this?
- How will I monitor this?
- How will I communicate this?
- How will I operationalize this?

If you can't answer all these questions for a given tolerance value, it's highly unlikely the value will be useful in terms of risk tolerance. If it can't be quantified, measured, monitored, and applied to processes, it will be difficult, if not impossible, to enforce.

Once these values are established both in subjective (appetite) and objective (tolerance) terms, they should become part of a normal reporting process, perhaps with a quarterly frequency. The table shows sample values to use as points of reference.

Soon we will address the process of socializing and incorporating these appetite and tolerance values throughout the organization. But first, let's consider some broad corporate governance aspects and then look at specific operational areas and see how these values might be incorporated into day-to-day activities.

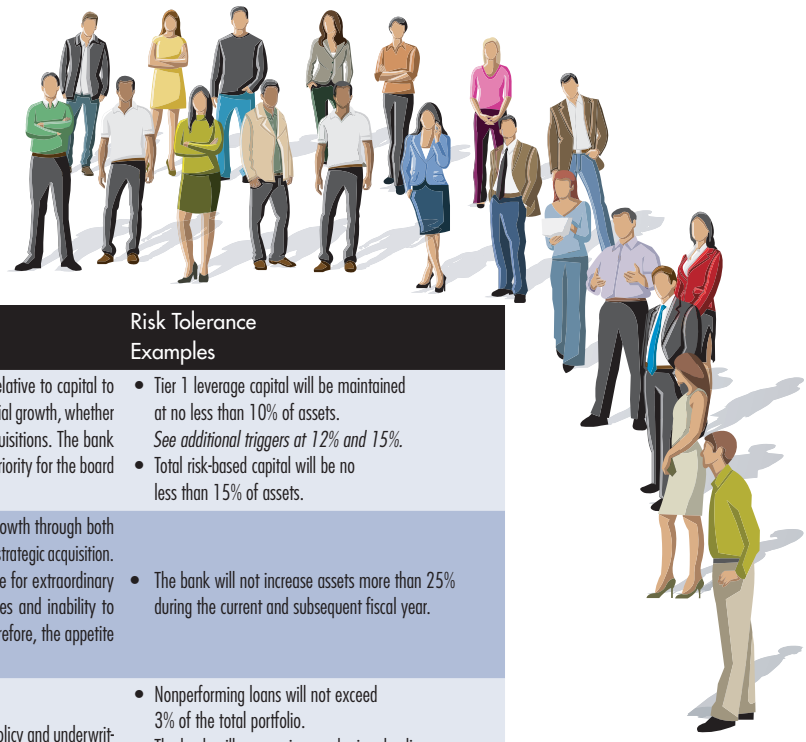
Governance Applications

Socializing Appetite and Tolerance

A risk tolerance that has not been communicated is effectively worthless. We can't criticize anyone for not following rules when we haven't said what they are. The goal of risk management is to help identify people's assumptions, and one of the most significant assumptions people hold is their perception of an acceptable risk level. Communicating acceptable levels is key to aligning operations with the overall intent of risk acceptance. Unfortunately, one of the quirks of human nature is that people often like to manage to their own risk appetite, and unless given specific direction they will do so to a level they find appropriate.

Communicating acceptable risk requires discretion. While some values can be communicated harmlessly throughout the organization, others may need to be disseminated more thoughtfully. Evaluate on a case-by-case basis to determine the right timing, level, and audience for communicating acceptable tolerance.

Training is one of the most important and straightforward ways to communicate risk tolerance. But often we train in



Business Category Examples	Risk Appetite Examples	Risk Tolerance Examples
Capital	The bank maintains a *low* risk appetite relative to capital to support existing operations and also potential growth, whether organic or achieved through strategic acquisitions. The bank remains well capitalized, which is a high priority for the board and senior management.	• Tier 1 leverage capital will be maintained at no less than 10% of assets. *See additional triggers at 12% and 15%.* • Total risk-based capital will be no less than 15% of assets.
Growth	The strategic plan for this year calls for growth through both organic means as well as the potential for a strategic acquisition. However, the bank has a low risk appetite for extraordinary growth owing to limited internal resources and inability to quickly expand internal infrastructure. Therefore, the appetite for growth risk is *low.*	• The bank will not increase assets more than 25% during the current and subsequent fiscal year.
Credit Risk	The bank's appetite for credit risk (credit policy and underwriting) is *low,* as reflected in its conservative credit policy and underwriting criteria. The bank will originate new loans only in industries where it has expertise and experience.	• Nonperforming loans will not exceed 3% of the total portfolio. • The bank will engage in no subprime lending. • Etc. *For additional lending risk metrics, see the bank's credit policy.*
Operational Risk (Technology)	The bank recognizes that while technology is critical to supporting bank operations, it is also susceptible to obsolescence and potential failure. Varying levels of fault tolerance and recoverability have been built into key systems; however, other less critical systems do contain single points of failure. Therefore, the bank's overall appetite for information technology risk (as a part of operational risk) is considered *moderate.*	• No system will remain in production more than one year past its scheduled amortization date. • All mission-critical systems shall maintain uptime of not less than 99%.

the "dos" and "don'ts" of a job, never saying *why* a practice is important. For managing risk, the *why* really is important. Only when people appreciate the underlying goal—whether it's to create value or mitigate risk—can they share ownership in the process. Managing a control is not the same as managing a risk. To effectively manage risk, we have to give people the context for the control.

Risk Assessments

If the goal of a risk assessment is to evaluate that risk against the context of risk appetite, we need to have assessment tools that support our appetite and tolerance intentions. For example, we may choose to establish tolerance values for capital risk or strategic risk, which means we need assessment tools that assess risk to capital and strategy (macro-level risk profiles). Assuming we also have established an acceptable risk profile for operational risk, then we also will need tools for assessing that risk at a more process (or micro) level. What this means is that a sound ERM framework needs to be implemented in a way that allows us to assess at a macro (strategic) level as well as a micro (operational) level because different appetite and tolerance values will apply at different levels.

For operational assessments, it's critical that we be able to assess risk in terms of *processes* because our processes are the known quantities and the means by which we actually manage risk. (No one manages only one risk type; they manage a process.) However, to tie back to risk tolerance, we have to be able to assess the embedded risk types within a given process (such as credit risk). This assessment creates a challenge for risk managers, but it's not insurmountable. As long as assessments remain grounded in the underlying processes but allow the assessor to consider the implications of an operational event across the range of risk types, we can accomplish both the functional risk assessment and the assessment by risk type.

If the goal of a risk assessment is to evaluate that risk against the context of risk appetite, we need to have assessment tools that support our appetite and tolerance intentions.

Change-Management

Managing change is one of the most powerful and profound ways to operationalize risk tolerance. Again, the seeds of risk are sown in change, and the best place to ensure risk

alignment is in the design phase.

Change always involves three key considerations:

1. What is the business benefit?
2. What is the cost?
3. What is the risk?

People love to talk about the benefit, they tolerate discussion about cost, and they avoid or downplay the risk like crazy. Once the project sponsor has become emotionally committed to the idea of the benefit, he or she often regards an honest assessment of risk as unwanted negativity. Only when we analyze prospective change thoughtfully and transparently across all of these aspects do we have a real opportunity to compare change against acceptable risk levels.

It's up to management to evaluate each area of lending and determine whether it conforms to overall risk appetite.

We have to consider how change is proposed, vetted, and approved. Who is involved and do they have a crystal-clear sense of what acceptable risk looks like? Are we being honest with ourselves about the benefit, cost, and risk? Do we understand the internal implications of the change, or are we so fixated on the benefit that the rest is pushed to the back? Finally, are the tools and methods provided to our business units designed so that the assessment results can be compared to risk-tolerance levels? Can informed decisions be made about whether the change represents an acceptable level of risk?

Functional Applications

Let's consider some practical applications of operationalizing risk tolerance. In each of these cases we'll explore foundational aspects of the operation and consider ways to turn high-level tolerance statements into specific operational methods and metrics.

Lending

In general, lending is one of the easier areas for operationalizing risk tolerance because many top-of-the-house tolerance values translate easily into individual limits and controls. In addition, lending is also a slower-moving area than, for example, deposits or electronic banking. However, some analysis may be warranted to determine how individual limits should be established. Consider these specific issues:

- If bank-wide limits have been established for, say, *concentration risk* (products, industries, etc.), management may need to evaluate the aggregate of projected origination across all loan officers, compare that with current portfolio concentration, and set individual product limits accordingly. Again, lending doesn't usually move quickly, so this could be accomplished through individual limits or aggregate portfolio monitoring.
- Where *credit risk* tolerance levels are set for the portfolio overall, they will need to be consistent with the judgmental underwriting criteria given to individual loan officers.
- Where low tolerance levels for *compliance risk* usually are established at a bank-wide level, they must be reflected within specific operating controls and monitoring mechanisms that let people at the operational level know what is expected.

In general, it's up to management to evaluate each area of lending and determine whether it conforms to overall risk appetite:

- Do individual limits reflect overall credit and concentration risk tolerance?
- Does the aggregate of limits consistently reflect overall risk appetite?
- Do sales incentives align with risk appetite?
- Does everyone really understand operational risk?
- Does the credit staff see beyond credit risk?

This task is not difficult, but it must be done deliberately and thoughtfully to ensure no surprises come from inaccurate assumptions. Too often, lending is managed instinctively rather than by careful, detailed analysis of whether the aggregate of all loan origination, underwriting, and back-office operations reflects intended overall exposure.

Information Technology

One of the biggest areas of disconnect between board-level risk appetite and actual operational risk levels is information technology (IT). How the board—and often senior management—sees the risk profile is often very different from reality. Three primary issues exacerbate this problem:

1. IT staff speak one language, a largely technical one, and management speaks another. To the extent that this gap is not resolved, risk will exist.
2. IT and executive management often have very different risk-tolerance levels. Management wants IT systems up at all times without fail. IT knows that everything breaks eventually; it's only a question of when. But IT also knows that when something does break, it can be fixed. A problem exists when there are differences in understanding fault tolerance and recoverability.
3. Unspoken assumptions—the heart of all risk—are rampant. They include assumptions about system sufficiency to support the business, fault tolerance, staff capabilities, obsolescence, and security. Effective risk management recognizes these assumptions and ensures everyone is in agreement.

To effectively translate bank-wide operational risk tolerance for IT into operational controls, the following tools are needed:

- ***A strategic technology plan—***This is the important element in operationalizing IT risk tolerance, and yet far too many institutions don't have a detailed, comprehensive

plan for technology used to support the business. This effort should include a detailed, one-year plan and an abstract plan for years two and three. It should fully reflect initiatives and objectives outlined in the corporate strategic plan—specifically, which technologies will be purchased, upgraded, or replaced. It should also clearly indicate what will be done to support the existing infrastructure, regardless of whether these technologies are tied to specific initiatives. And finally, for all significant expenditures, it should clearly outline the benefit, cost, and risk of all proposed technologies. The aggregate of the risk analysis contained within the strategic technology plan—which represents proposed change—combined with the IT risk assessment that management conducts on existing internal systems is the collective risk profile. If this information does not match bank-wide statements about operational risk for technology, something is wrong and must be adjusted.

- ***Risk metrics—***To report on the state of the IT infrastructure, IT needs clearly defined metrics, many of which are probably already in place. Management needs to evaluate which of these metrics will be reported to the risk committee and senior management as evidence of compliance with the overall risk appetite. Examples may include systems reaching obsolescence, load factors, average downtime, and so on. The real key is that metrics may be backward-tracking (telling you something that has already happened), but reporting needs to be forward-looking (telling you what you should believe it means about future performance). It's the latter, not the former, that's usually correlated with risk appetite.

- ***Risk monitoring—***Similarly, management needs proper monitoring mechanisms to ensure that the systems infrastructure is operating within acceptable tolerance levels and recoverability standards are being met. Examples may include key system status and IT project status.

- ***Capability analysis—***As organizations grow, it's important to periodically reassess whether staffing and skill sets are sufficient to support the organization. Institutions should have bank-wide statements outlining required staff levels and capabilities in line with expected growth, and management should determine if these requirements are being met. Whether this analysis is done annually or every two or three years is up to the institution and will depend largely on the firm's growth rate and staff turnover.

- ***Language lessons—***Executive management and IT must be able to communicate effectively about risk appetite. Executive management may not believe that it's imperative to understand the inner workings of the firm's technology environment, but really it is. If members of senior management don't have at least a working understanding of how the business is being supported and what the IT risk profiles are, it will be impossible for them to attest that the institution is operating within acceptable tolerance levels. They will be taking the CIO's or someone else's word for it, and that's poor management. If the CIO is incapable of articulating the overall risk profile for the technology infrastructure in business terms, then he or she has no business being CIO.

Operationalizing risk tolerance into the IT environment means coming to a common understanding about the systems infrastructure and related risk profile, agreeing on risk levels at every level of the organization, and getting all unspoken assumptions out in the open so they can be discussed and managed together.

Information Security

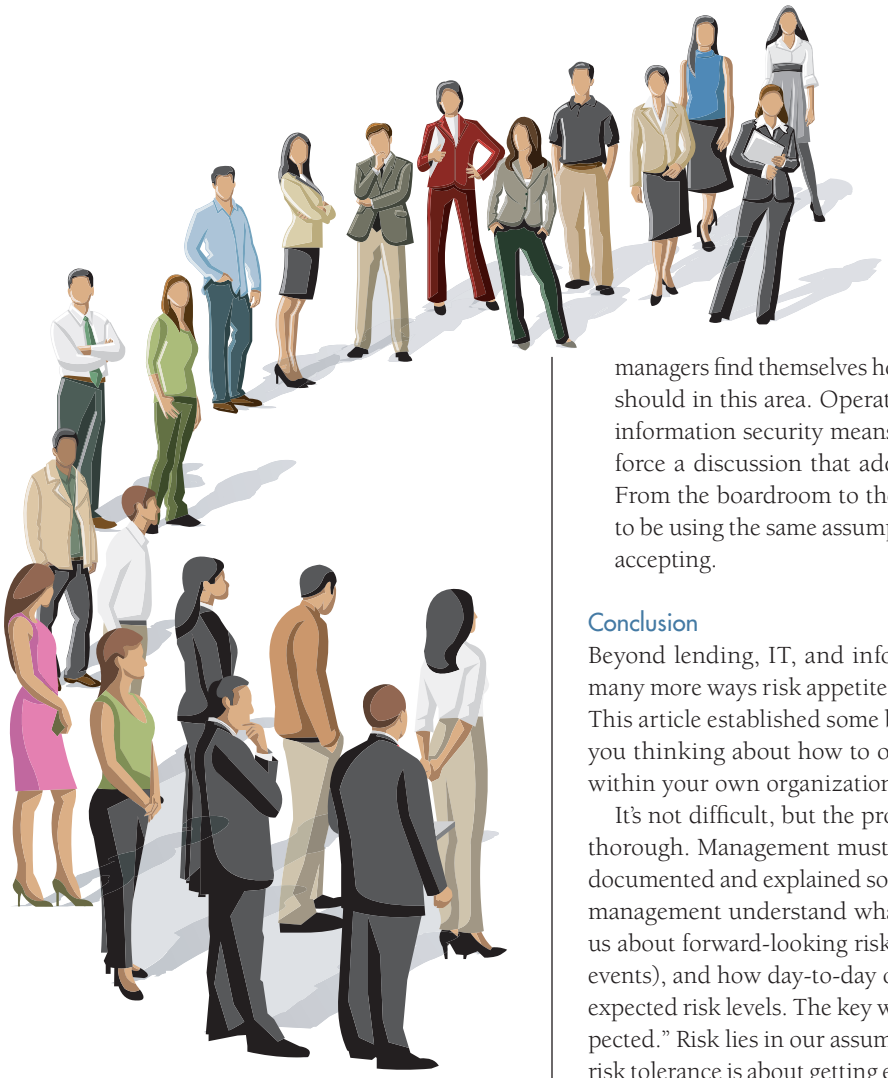
Information security is another area where we see a profound and, at times, staggering disconnect in risk tolerance. If you ask CEOs or board chairs about their tolerance for information security risk, they will almost always answer "very low" because they generally understand the consequences of a major data breach.

If you ask your CIO the same question, the answer you will get is "moderate to high." The CIO knows that there are dozens, hundreds, or even thousands of employees with direct, unrestricted access to confidential customer information, along with hundreds of (or more) third parties that require customer information in order to provide products and services to the bank. Your CIO also knows that, despite strong controls to protect data, if people were truly determined to steal customer information, odds are they could. You live with this risk in order to conduct business. The disparity between what executive management wants as its risk profile and what management *knows* is the risk profile must be addressed. Everyone must agree about what is an acceptable amount of risk. That's why it's called risk alignment.

The disparity between what executive management wants as its risk profile and what management *knows* is the risk profile must be addressed.

To achieve risk alignment and successfully operationalize information security risk, you must do the following:

- Have a realistic and comprehensive *risk assessment* process and tool to establish and articulate a true risk profile. But—and this is critical—this means looking at more than IT systems. Internal systems are just part of the overall risk profile. You also have to look at data sources (which are owned and managed by business areas), third



parties, and physical records. The result of this assessment, if comprehensive enough, should outline in clear terms for the board and senior management the *actual* information security risk profile. This result must match the appetite and tolerance levels articulated at the top of the house. If not, something is wrong and has to change. Either more controls are needed to bring the profile to a lower risk level, or executive management has to accept life with a moderate-to-high risk profile.

- Require deep, honest discussions to help staff truly understand and appreciate risks, as well as what needs to be done to minimize them. Most companies are far too liberal in granting access to data and far too complacent when it comes to monitoring access both internally and externally. A common understanding about a risk and each individual's responsibilities in protecting data will enable you to align that risk with expected overall tolerance levels.
- Dig into the facts and address them head on. Data security scares executives. Too many board members and senior managers find themselves hoping they're doing what they should in this area. Operationalizing risk tolerance for information security means we get past these fears and force a discussion that addresses the real risk profile. From the boardroom to the basement, everyone needs to be using the same assumptions about the risk they are accepting.

Conclusion

Beyond lending, IT, and information security, there are many more ways risk appetite needs to be operationalized. This article established some basic design principles to get you thinking about how to operationalize risk tolerance within your own organization.

It's not difficult, but the process must be deliberate and thorough. Management must ensure that risk metrics are documented and explained so that the board and executive management understand what they mean, what they tell us about forward-looking risk (not just backward-looking events), and how day-to-day operations are conforming to expected risk levels. The key word in that last phrase is "expected." Risk lies in our assumptions, and operationalizing risk tolerance is about getting everyone's assumptions in the open. That way, we can act together to determine where they are out of alignment and what we're going to do about it.

Only when we are operating with a shared set of assumptions do we have any chance of ensuring alignment between the high-level risk appetite statements and what actually happens in the inner workings of the company. This is what risk *management* is about—and where we need to go. One of the worst assumptions we can make is that people within the organization "get" management's intentions for risk tolerance. They don't. ❖

Eric Holmquist *is managing director of enterprise risk management advisory services for Accume Partners. He can be reached at* eholmquist@accumepartners.com.

Notes

1. To guide its members in the process, RMA published a risk appetite workbook in 2012. For details, visit the RMA website (www.rmahq.org).
2. "Operationalize" is a made-up word. Its intended meaning here is what one might expect—the process of applying global principles to specific operational processes.