The use of key risk indicators (KRIs) as a risk management practice and business support tool is evolving rapidly, if not awkwardly, within the financial services industry. While the concept makes sense and easily fits within a risk governance framework, the practical application and cultural acceptance of KRIs face challenges at institutions of every size and composition. Different approaches to the design and execution of a KRI program have met with varying degrees of success, but we can’t yet point to any particular model as a “best practice.” While recent case studies highlight more and more success stories, there is no question that opportunities exist for improvement and further refinement.

Small to medium-sized institutions (SMSIs) often learn from the successful strategies of larger institutions, but they can’t do that with KRI implementations. It’s simply too early in the KRIs’ life cycle to extract meaningful design characteristics from others’ efforts. However, SMSIs should pursue their own KRI programs because even basic KRI deployment to limited functional units can improve risk management practices through increased risk awareness and accountability. A sound KRI framework strengthens the overall risk management program by:

• Providing improved risk awareness and early warning metrics.
• Allowing for more proactive risk management rather than reactive.
• Reducing both expected and unexpected losses.

Developing Practical Key Risk Indicators for Operational Risks in Technology

This article explores the issues and opportunities for small and medium-sized institutions pursuing a basic KRI structure for technology risks.

BY ERIC HOLMQVIST
The issues and opportunities for SMSIs pursuing a basic KRI structure for technology risks include:

- Identifying operational events involving technology that historically have had a substantial impact.
- Reviewing methods used within organizations today to assess technology risk.

Some key questions to consider:

- Are these efforts centralized, decentralized, or some combination of both?
- Are technology risks assessed separately from operational risks?
- What technology-based risks are considered both from an infrastructure/environment perspective (e.g., capacity requirements), as well as from an application perspective (access or login ability)?
- What can be meaningfully measured, and do those measures translate into business risks?
- What would it take to develop a program of KRIs relative to the technology that drives the business process?
- Is there a discrete set of KRIs that represents the essence of technology risk?

### Risk Indicators for Technology

Establishing risk indicators for technology-centric risks is a valuable management technique, yet it’s one that’s difficult to set up. Challenges include:

- Management awareness.
- A willingness to manage reactively.
- Difficulty in determining practical metrics, resource constraints, and vague correlations between metrics that can be tracked and specific risks.

In addition, many significant technology-related events occur so quickly they do not present advance warning signs. Also, activities that use extensive or complex technology may experience an operational failure because of human error. In this case, the technology may create a leveraging of the risk, but is not the source of the risk itself.

Nevertheless, the industry has become irreversibly dependent on technology for all bank operations. That’s why the industry must continually develop and improve technology-based KRIs, which would provide lead time before an emerging event, or at least indicate an increased risk profile. This article identifies a number of specific risks and indicators that are measurable and can be correlated to risks. However, each institution will have to evaluate KRIs that are appropriate and practical for its own operation based on its composition, complexity, and available resources. SMSIs face significant challenges when they attempt to design and implement a KRI program, particularly one that addresses technology KRIs. The connection between technology-based metrics and potential business risk is not always clear and then you add on top all of the events that cannot be measured.

Ironically, even the smallest of institutions already use a wide variety of basic risk indicators to measure and monitor hundreds, if not thousands, of moving parts daily through logs, reports, databases, alarms, and good old-fashioned gut instinct. Many of these measures are tied to pre-established threshold values that may trigger certain actions to be taken. In some cases, even the underlying potential risk associated with an indicator is known and communicated.

The banking industry has perpetuated a remarkably stable operating environment using all of these tools and techniques, so it surely should be able to identify those precious few metrics, the illuminati of indicators, that can mean the difference between expected losses and unexpected losses, or even the life or death of the institution itself. And yet the concept of establishing a discrete set of key risk indicators remains paradoxically elusive, particularly as it relates to technology.

RMA’s KRI Library is an example of an industry initiative to standardize indicators, but many challenges must be tackled by the institution itself. Discussed below are some unique challenges that may inhibit the development of a KRI program at SMSIs.

### Management Challenges

What are some of the challenges that may inhibit the development of a KRI library within financial institutions?

- **Lack of standards and best practices**—For better or for worse, the SMSIs look at the many operating methods and controls used successfully by other institutions. The SMSI often scales for its environment the more advanced management techniques of larger institutions. Until KRI practices mature and become time-tested, each institution will have to continue experimenting with different risk indicators to determine which are effective and manageable.

- **Management awareness**—The control measures that get the most attention and support are those that senior management understand and expect. Because the concept of an enterprise-wide KRI library is still very new to the industry, many senior managers are unaware of...
its value, let alone its design, so they are hesitant to allocate scarce resources to develop such a program.

- **Speed of change**—Technology changes at an extremely rapid pace, so risks that may be imbedded or inherent within a given technology today may increase or decrease with successive versions or developments. KRIs that are linked to a specific technology or even technology-centric process need to be routinely reevaluated any time that the underlying technology goes through a major revision.

- **Control measures**—Before effective KRIs can be designed and implemented, the institution must be able to clearly establish its internal control measures. An organization that is not confident in its control measures cannot build “status” measures around them. Fortunately, many institutions have gone through extensive exercises to document key control measures as a part of their compliance programs, particularly those subject to the Sarbanes-Oxley Act. These controls often serve as the foundation for determining active risk indicators.

- **Lack of a process “decay” period**—Some aspects of technology can be effectively monitored for subtle changes or degradation. Others defy monitoring. They can move very quickly from a stable state in which nothing is happening to one of dramatic change. For example, the lack of any computer viruses on the internal network can be routinely monitored, but a virulent computer virus that suddenly penetrates the network’s defenses can’t be measured by a KRI since the environment would go immediately from “stable” to “bad,” completely bypassing “trending toward bad.”

- **Technology versus risk focus**—People charged with implementing and maintaining the bank’s technology are, for the most part, focused on the technology itself and not necessarily the business risk associated with a potential failure of the technology. The development of technology-based KRIs is probably going to require the development of more mature communication channels between the subject matter experts regarding what could go wrong with the technology and what that would mean to the business.

- **Technology versus process risk**—Processes dependent on technology must include the potential failure of the technology as a risk. In failure scenarios, there is a gray area because the failure could be due to the technology itself or to how the technology is used.

  For instance, if the mis-configuration of an externally facing router exposes the bank’s network to the public Internet, is that a technology risk or a process risk? Many technology-centric KRIs may only make sense within the context of a full KRI library to cover all operational risk areas.

### Fundamental Questions

On balance, this plethora of seemingly insurmountable challenges and inhibitors raises a number of fundamental questions about the idea of a technology-centric KRI, including:

- Are they practical?
- Are they manageable?
- Are they even feasible?
- Can they exist without a comprehensive assessment of all operational risks?
- Can risks truly be mapped to metrics when it comes to technology usage?
- Is technology simply too complex and too fast-moving to be managed with KRIs?
- Is the focus ever really on a technology, or is it on the process that it supports?
- Do changes to technology (new systems, upgrades, etc.) substantially invalidate existing KRIs to the point where the whole KRI library must be rebuilt every time technology is changed?
- When will best practices emerge, if ever?

Going beyond these very tactical, pragmatic questions, there is one transcendent question that looms large and strikes at “the very nature of things”:

> Do we actually manage the technology that supports a business operation by instinct? Despite all of the strategic planning, design specifications, implementation strategies, and systemic and procedural controls, do we manage the really big risks and then deal with the rest if and when they come up? Is that how we must manage given the basic nature of technology and IT staff members, and given the inherent complexities and unceasing change?

In short, the answer to those questions is that mapping KRIs to technology usage is not an insignificant task. It requires a great deal of creativity, cleverness, cooperation, and (for lack of a better word) contempt for passive management. It will probably take years to fine-tune the practice of developing KRIs for technology, and the effort will require creative insight from many sources both inside and outside the industry. However, KRIs today are a powerful management technique that institutions can use to manage proactively, reduce losses, minimize operational impacts, and increase return on investment.

### What Is a Technology-Based KRI?

Despite profound challenges and uncertainty of success, we pursue technology-based KRIs because we know they
With the growth of credit portfolio management and the approach of Basel II, you need the knowledge and skills to assess whether this approach is right for your bank. This popular RMA course will help you:

- Weigh the many benefits of credit portfolio management.
- Evaluate probability-of-default models.
- Determine the data you need and how to assess your sources.
- Measure the risk contribution of an individual transaction.
- Estimate the economic capital required to support a portfolio of credits.

For more information, or to register, please visit www.rmahq.org/RMA/CreditPortfolio, or call RMA Customer Care at 1-800-677-7621.

Credit Portfolio Management Workshop

Learn how to take a portfolio approach to managing your bank's credit risk

June 3-4, 2008
InterContinental Harbor Court
Baltimore, Maryland

RMA is Proud to Announce the Latest Credit Risk Certified Designees

Roger E. Anderson  Sarah K. Gill  R. Bruce Knox  Glenn R. Sellen
Katherine S. Armstrong  Trenton K. Gorman  Carrie L. Kosac  Jason A. Smith
Edward T. Borchert  Amie Gunderson  Judd P. McNally  Kevin M. Stacey
Rachel Breashears  Brian C. Haddock  Jon Mensie  Crystal Taylor-Baker
Amy M. Chubbuck  Matthew S. Hammond  Mark S. Novak  John A. Teshima
Peter C. Eberhardt  Dawn A. Howard  Russell L. Packer  Paul D. Tipps
Kevin D. Eckerty  Lindsey B. John  Stephen P. Panagouleas  Kristina J. Walker
Susan S. Eldred  Timothy A. Johnson  Scott J. Pate  Kari L. Weiter
Mark A. Franklin  Christopher Johnson  Scott Peterson  Brad L. Wells
Jenni M. Frazer  Jeffrey R. Kaiser  Edward R. Polli II  Tim West
Noah Frient  Matthew L. Kind  James Richardson  Peter A. Yanief
Gregory J. Gibson  Matthew T. King  Denise D. Rule  David M. Zieno

www.rmahq.org/RMA/CRCDesignees
Enhance risk governance. Well-designed KRIs make risk assessments dynamic and fluid by capturing subtle or not-so-subtle changes in the operating environment that could influence risk profiles.

Before reviewing the list of KRIs that was identified in the course of this research, some basic design principles should be discussed that focus on practicality and efficiency. A number of industry treatments have been previously published on KRIs in general, and these principles will not be repeated within this article. There are, however, a few worth repeating and some that are specific to technology-based KRIs that should serve as an addendum to these other works. The principles are as follows:

- To the extent possible, focus a technology-based KRI on a specific technology or technologies, not on how a technology is used. KRIs that may indicate a process failure are also valuable, but should be part of the process KRI list, not a technology KRI list.
- When designing KRIs, be careful to distinguish between potential issues and a perception of potential issues. For

<table>
<thead>
<tr>
<th>Business Risk</th>
<th>Metric</th>
<th>Risk Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology sufficient to support business</td>
<td>Level of IT funding relative to industry.</td>
<td>IT spending that is inconsistent with industry standards, particularly relative to security, will ultimately create strategic and operational risk to the bank.</td>
</tr>
<tr>
<td></td>
<td>Changes in industry demand for a given technology or number of providers.</td>
<td>Notable changes may indicate obsolescence of the technology.</td>
</tr>
<tr>
<td></td>
<td>Number of failed (did not meet business objectives) or abandoned IT projects.</td>
<td>Possible indication of insufficient management or strategic technology plan linking business needs to technology solutions.</td>
</tr>
<tr>
<td>System integrity and availability</td>
<td>Number and scope of system failures over a certain magnitude.</td>
<td>Increased frequency of failure likely indicates deeper issues with system integrity or management.</td>
</tr>
<tr>
<td></td>
<td>Network storage utilization.</td>
<td>Utilization over threshold amounts may create risk of depleting storage space and operational impact.</td>
</tr>
<tr>
<td></td>
<td>Number and scope of failed system changes.</td>
<td>Frequent or significant failed system changes can be directly correlated to insufficient change-management practices.</td>
</tr>
<tr>
<td></td>
<td>Erosion of technology vendor profile, including reduction in frequency of upgrades, diminished support levels, or significant staff or management changes.</td>
<td>May indicate the potential for loss of technology or support for that technology.</td>
</tr>
<tr>
<td>Data confidentiality</td>
<td>Frequency of requested change to system access rights.</td>
<td>The more people who are given access rights to data, the higher the risk of compromise. Significant increase in access requests may also indicate potential internal fraud.</td>
</tr>
<tr>
<td></td>
<td>Number of portable devices utilized.</td>
<td>Each increase in the number of approved portable devices (laptops, flash drives, PDAs) creates incremental risk.</td>
</tr>
<tr>
<td></td>
<td>Average time to implement critical system patches.</td>
<td>Any increase in average time to implement may create exposure to system resources and data.</td>
</tr>
<tr>
<td></td>
<td>Number of data breaches or near misses.</td>
<td>Any increase in either data breaches or near misses may indicate significant management or control failures.</td>
</tr>
<tr>
<td>Data integrity and availability</td>
<td>Frequency and success of tests to data backups.</td>
<td>Any reduction in testing frequency or increase in failure rates represents a significant increased risk as data back-ups are central to the business resumption strategy.</td>
</tr>
<tr>
<td></td>
<td>Number and scope of control issues identified by independent reviews (internal and external audit, and third-party vulnerability assessments).</td>
<td>Increase in number or scope of technology-related issues may indicate an increased risk to data protection.</td>
</tr>
</tbody>
</table>
instance, a user’s perception that the network is “running slow” is not a good risk indicator, but a system report that indicates that the system is reaching certain utilization thresholds is. People should not be discouraged from being observant (in fact, quite the opposite), but risk indicators should be based in fact.

• KRIs cannot be theoretical; relate them to a specific, measurable activity. However, in certain instances they may have to be based on a subject matter expert’s observation, such as a significant reduction in a vendor’s ability to support a product. In the end, the basis for the KRI must be defensible.

• To the extent possible, correlate KRIs directly to a specific risk, as opposed to postulating, “If x happens, then y could lead to z happening.”

• Early in the development life cycle of a KRI program, focus on measures that can be quantified. You do not want the advancement of the program to become bogged down in disputes over how to interpret a subject measure.

• Use a primary and secondary design structure with technology-based indicators. The primary response would be, “What do you need to do right now?” The secondary response would be, “What does this mean?” System failures are an excellent example. One-time failures will happen routinely and represent one form of risk (commensurate with the system that fails). However, repeated system failures indicate an entirely different form of risk with exponentially higher exposure. Therefore, the one-time failure may be treated only in the technology risk assessment, whereas the presence of repeated failures would be represented in a KRI.

• Consider key indicators that are meaningful to the size of the organization. For instance, network uptime is a meaningless statistic to all but the largest institutions. However, the number of discrete incidents that resulted in network downtime (and the trend over time) is a meaningful number.

• Follow the old SMART acronym—KRIs should be specific, measurable, achievable, relevant, and timely.

You can reasonably approach the design of KRIs for technology from two different perspectives because both ultimately lead you to the same place. One method is to consider significant risks to the business and then ask, “What can we measure that might indicate an increased risk?” (The answer should naturally lead to a mix of process and technology-based metrics.) A second method is to determine the systemic things that the institution can measure and track, given its available technology and human resources. (Examples may include failed login attempts, external attempts at unauthorized network access, etc.) Then you can consider whether that metric translates into a significant business risk. Evaluating technology-centric KRIs from both perspectives is a more holistic approach that considers both the impact and the ability to measure. All metrics have the potential to be a key risk indicator; it comes down to what a change in that metric “means” to the business.

Lists of technology-specific risks and KRIs are of the highest value to the SMSI and are considered highly manageable, practical, and correlated to specific business risks. Such lists may not be appropriate for all institutions and are subject to changes over time; however, they may serve as a starting point for establishing an initial list within the institution.

Conclusion

KRIs for SMSIs may never be standardized across the industry because each institution is slightly different and uses technology to different degrees. In addition, they may ultimately develop some or many KRIs that are subjective in nature and require some level of input from subject matter experts (e.g., health of a specific technology vendor or trustworthiness of a given employee). This is the nature of the beast in a smaller institution because one major failure can have catastrophic consequences, and advanced data measurement and monitoring systems may not exist. The process of developing a dynamic and comprehensive KRI library for institutions of this size will be challenging, time consuming, at times frustrating, and probably will require fine-tuning for years to come. However, the progressive institutions that pursue this advanced management practice will achieve a more stable working environment, be able to respond much more proactively to emerging threats, and earn a distinct competitive advantage over those institutions that continue to manage increasingly complex technology intuitively and reactively.

Eric Holmquist is director of operational risk at Advanta Bank. He can be contacted at eholmquist@advanta.com.