rma
THE RISK MANAGEMENT ASSOCIATION

RISK MEASUREMENT, EVALUATION, AND COMMUNICATION WORKBOOK

JOIN. ENGAGE. LEAD.

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

Risk Measurement, Evaluation, and Communication Workbook

THE RISK MANAGEMENT ASSOCIATION

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 management 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 18,000 individuals are located throughout North America and financial centers in Europe, Australia and Asia.

Members actively participate in the RMA network of chapters. These chapters are run by RMA Associates on a volunteer basis and they provide our members with opportunities in their local communities for education, training, and networking throughout all stages of their financial services career. Chapters are located across the U.S. and Canada as well as in financial centers internationally.

RMA members also avail themselves of benefits offered through headquarters in Philadelphia, Pennsylvania. To assist members in advancing sound risk principles, RMA keeps members informed and provides access to industry information at this site; publishes a journal (*The RMA Journal*) and a variety of newsletters, books, and statistics; conducts many workshops and seminars; holds several conferences, an annual convention (Annual Risk Management Conference); and has numerous committees working on a variety of projects.

RMA welcomes all personnel involved in lending and risk management in member organizations to become RMA Associates.

Note: As a not-for-profit, professional association, RMA does not lobby on behalf of the industry.

The information contained herein is intended for educational, informational, and research purposes only. You use this book and information at your own risk, and RMA assumes no responsibility or liability for any advice or other guidance that you may take from this book or the information contained therein. Prior to making any business decisions, you should conduct all necessary due diligence as may be appropriate under the circumstances. RMA assumes no responsibility or liability for any business decisions, including but not limited to loan decisions, or other services rendered by you based upon the Risk Measurement, Evaluation, and Communication workbook or results obtained therefrom.

For more information, contact the Customer Care Department by phone 800-677-7621 / Fax 215-446-4101 / or our website: www.rmahq.org.

TABLE OF CONTENTS

TABLE OF CONTENTS

ACKNOWLEDGMENTS

RMA wishes to acknowledge the work, thoughts, and contributions of the Risk Measurement, Evaluation, and Communication Workbook working group. To the members of this group, RMA extends its appreciation.

Group members		
James Costa	Chief Risk Officer and Chief Credit Officer	TCF National Bank
Caleb Dupuis	SVP / Director of Enterprise Risk Management	First United Bank & Trust Co.
Ronda Edkins	EVP / Enterprise Risk Manager	PNC Bank NA
Thomas O'Hara	EVP / Enterprise Risk Management Director	Huntington National Bank
Joseph A. Iraci	Managing Director / Financial Risk Management	TD Ameritrade
Sandeep Jadeja	ICAAP Analyst II	MUFG Union Bank NA
Joseph Martony	Chief Risk Officer	Los Alamos National Bank
Jennifer O'Reilly	VP, Director of Enterprise Risk Management	First Republic Bank
Edward P. Schreiber	EVP / Chief Risk Officer/ Head of Enterprise Risk	Zions Bancorp
Kevin Slane	Director of Enterprise Risk Management	Hancock / Whitney Bank
Jonathon W. Trowbridge	Head of Risk Control and Quantitative Modeling	Green Plains, Inc.
Warren W. Woodring	EVP / Head of Wholesale Risk	SunTrust Bank
Kenneth K. Yoo	SVP / Chief Risk Officer	Federal Home Loan Bank of Atlanta

SPECIAL THANKS

We also extend a special thanks to Eric Holmquist, Managing Director, Risk Solutions Group at FIS, for content contribution, technical advice, and practical insight.

Eric is an active supporter of RMA. His work with RMA over many years has covered a wide range of enterprise and operational risk subjects.

Eric has authored articles for *The RMA Journal*, led round table and conference presentations, delivered audio-conferences, and served as a valuable member of *The RMA Journal* Editorial Advisory Board.

PREFACE

In 2008, RMA's Enterprise Risk Management Council embarked on an effort to create an enterprise risk management (ERM) framework that banks could use to understand and manage the risks throughout their organizations.

ERM is the capability of an organization to understand, control, and articulate the nature and level of the risks taken in pursuit of a risk adjusted return.

The risks can be categorized as credit, liquidity, strategic/business/reputation, market, operational, compliance/legal, financial, and capital adequacy.

This framework applies regardless of an institution's size or how it wishes to categorize its risks.[1] The circular depiction of the framework is intentional. The individual components (such as coverage or risk appetite) are not meant to be sequential, but rather to represent a dynamic flow in both directions. Culture is depicted as the center or heart of the program, since without the right culture, the other components are of dubious value.

After devising the ERM framework, the RMA ERM Council began developing a series of practical workbooks to guide risk management professionals as they implement the framework. The workbooks are:

1. *Risk Appetite* (published 2010)
2. *Governance and Policies* (published 2013)
3. *Risk Measurement, Evaluation, and Communication* (addressed in this workbook)
4. *Scenario Analysis and Stress Testing for Community Banks* (published 2012)

This workbook, *Risk Measurement, Evaluation, and Communication*, addresses 1) the mechanisms available to size risks in order to compare them to each other and to prioritize risk mitigation activities, 2) the strengths, weaknesses, and limits of each approach, 3) the "watch-outs" that are especially important when sizing, 4) the output that will ultimately be needed for the next step (response), and 5) the best ways to communicate the results.

1 Although there are similarities between the ERM frameworks developed by RMA and COSO, RMA's frame work is highly specific to financial services and offers guidance on practical implementation.

What Is ERM? It is the capability to effectively answer the following questions:

- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

INTRODUCTION

An indisputable tenant of risk management is that one must understand risk in order to manage it. Understanding risk requires the ability to quantify a given risk so that mitigating controls can be put in place to reduce the risk to an acceptable level, a level that is in line with the organization's risk appetite framework. Without the ability to effectively quantify risk, no risk program can be successful. Assessing risk, however, is not a simple task. Anyone who has ever performed a risk assessment knows that they can be notoriously difficult, some risk types more so than others.

When conducting risk assessments, what are we trying to accomplish? Whether we are performing an enterprise risk assessment, operational risk assessment, information security, compliance, BSA[2] , or any other type of assessment, our goal is to:

- *Identify unknowns*. Ask probing questions that might unearth new information about possible risks or even risk treatment options.
- *Document assumptions.* Risk always lies in the assumptions people make, and a good risk assessment will go a long way towards getting those assumptions out in the open where they can be scrutinized, challenged, and ultimately, agreed upon.
- *Create ownership.* The process of assessing risk, done correctly, should identify the players involved in impacting that risk and serve as a basis for assigning responsibility towards managing and mitigating that risk.
- *Right-size controls*. Effective risk management is not just about what can go wrong. It is about determining if there is a better way. In other words, if you're going to look at a process from a risk perspective, you should also consider if it is a good process. If risk assessments aren't leading to honest, introspective questions about how processes could be improved (particularly end-to-end processes), then you are either not asking the right risk questions, or you are not encouraging people to be candid enough in their own self-evaluation. Risk sizing is as much about efficiency as risk mitigation.
- *Align risk.* Finally, by identifying and quantifying risk, our goal is to ultimately align risk levels with those established in the risk appetite and tolerance framework.

Too often "risk management" is viewed as another type of control, or worse, a compliance exercise—a periodic process outside of our day-to-day duties. It is much more critical than that. It is sometimes said that strategic planning is about the most effective way to make a dollar, and risk management is about the most effective way to keep as much of that dollar as possible. Just as we need to understand where we are going strategically and the various options available to use with different possible returns, so we must also understand the risks we face and the opportunities to align that risk to acceptable levels.

2 The Bank Secrecy Act (BSA), otherwise known as the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Reporting Act of 1970 (31 U.S.C.5311 et seq.

Assessing risk is a challenge. As you dig deeper, you realize there is no one right way, no easy answers, and no universal assumptions. Some common challenges include determining:

- The best method to assess risk from among the different methods available.
- Whether the assessment should be qualitative, quantitative, or some combination of both.
- Whether you have enough data to perform a meaningful assessment.
- If you have enough resources to facilitate a comprehensive risk assessment.
- Whether you can build a framework that effectively neutralizes people's natural biases.
- Whether you can quantify risk in a way that can be evaluated directly against risk appetite.
- What happens when people disagree on what the risks are or on the effectiveness of the controls in place or what level of residual risk (risk appetite) is acceptable.
- How to get people to focus on doing risk assessments when they already have a full time job and are likely feeling burdened by the 15 different risk assessments they are asked to conduct?
- How to get people to actually invest in the assessment process and not just tell you whatever they think will make you go away?
- If your culture is one that doesn't ever talk about risks or vulnerabilities and if staff fear being penalized for raising risk issues.

Assessing risk is not easy. It is not quick. It is not obvious. Surprisingly, it isn't always meaningful. But it is critical to effective risk management in that it increases people's awareness of risk and their responsibility to manage it. Frustrating as it can be at times, it is a worthy cause.

It's important to find a workable balance between what can (and should) be assessed, and what can be "managed as we go." In other words, how much do we need people to quantify risk versus just using their intuition? Each institution must decide the answer to that question based on the institution's risk appetite (the risk they are willing to accept). The goal of this workbook is to go through sound, proven techniques for conducting risk assessments that are practical, manageable with limited resources, scalable, and provide meaningful information to help the institution manage itself more effectively. These tools and techniques will help your institution design a risk assessment framework that is appropriate for your size, complexity, structure, and capacity.

Most companies have, or are creating, a comprehensive risk appetite statement. As such, it is critical to understand the collective residual risk associated with the firm's business activities. Working through the process is not easy given that residual risk is a function of inherent risk, control design and placement, and control effectiveness. Further complicating the process is the need to normalize disparate risk types that are not intuitively similar, for example, credit and compliance risk. The rewards of successfully measuring risk(s) on a common scale are significant and imperative if a company is to oversee and manage risk in an effective manner. Not only will the company know which risk mitigation efforts to prioritize, but it will also be able to cascade aggregate risk (through limits) to its business units, thereby ensuring that no one unit's limits breach impacts the firm's overall risk profile. Finally, understanding the individual and aggregate risks of the firm allows for more fact-based discussions around capital, earnings, and liquidity at risk.

In this workbook, you will learn alternative approaches to sizing risk; however, any approach should consider the following three factors:

- Severity: What is the impact if the risk materializes?
- Likelihood: Given the risk scenario, what is the likelihood that it will happen?
- Frequency: Given the risk scenario, how often could the risk materialize?

In addition, you will learn how to use the risk measurement process to create risk metrics, which ultimately inform the risk appetite. Included in this workbook are examples of risk metrics by type that may help in developing or augmenting your specific risk appetite statement.

Undoubtedly, the process will be challenging as some risks are easily quantified while others are not. In the following chapters are tools that, when combined with internal discussion, debate, and challenge, will help you create a sustainable methodology for consistent risk measurement.

II. REEXAMINING END-TO-END RISK MANAGEMENT PROCESSES

Every risk manager worries that something will be missed. Countless hours are spent thinking of all the different ways that a significant risk could go unnoticed and manifest itself. The key is to establish basic risks to be measured with the understanding that this will be a fluid process, and you will always have the opportunity to make adjustments later. Do not overthink the process. You will be better off first getting this process established. This section looks at ways to reexamine your end-to-end risk management processes to find the weak spots.

RISK IDENTIFICATION

To start challenging your risk management framework, begin with the risk identification process itself. Do you have a comprehensive and repeatable process to identify material and nonmaterial risks throughout business lines, products, and services? Risk identification is the first step taken by independent risk teams (the second line of defense) working with business-line experts (the first line of defense). These discussions are crucial to downstream efforts on sizing, setting limits, monitoring, controlling, and reporting risks. Not identifying risks correctly at this stage could affect your ability to size the risks correctly, set limits, and monitor the results. Risk teams need to maintain clear lines of communication on changes affecting the first line and, where possible, establish continuous monitoring of risks. Without the fluid exchange of information, the effectiveness of the second-line independent risk teams to capture all significant risks and manage them could erode. The risk identification step is foundational to understanding the complexity of risks that exist on an institution's books and in its products and business activities.

RISK MEASUREMENT

Once risks are identified, management has to allocate its scarce resources to measuring risk and optimizing the measurement approaches to cover the largest and most complex risks. Resource allocation has remained a challenge for management given the changing nature of risks and the environment. Management also has to find the right balance between the level of investment and the complexity of risks faced by an institution. Too much investment in one area could lead to too little in another, potentially causing a significant risk to be overlooked.

Assessing the complexity of risks gives management a better understanding of the amount of resources to allocate. The complexity of risks can depend on multiple factors, such as the mix of products and services, lines of businesses involved, and market factors. There are also numerous approaches to measuring and understanding the complexity of risks, each with its own set of benefits and weaknesses.

III. RISK ASSESSMENT PRINCIPLES

Before exploring techniques in conducting risk assessments, it's important to understand the basic principles that will help the institution determine the most appropriate framework for its purposes.

Focus on key risks.
For enterprise and operational risk assessments, focus on key risks versus non-key or routine risks. Or, as Rick Parsons describes it in his book *Broke: America's Banking System, Common Sense Ideas to Fix Banking in America*, "Major in the majors." For enterprise and operational risk assessments, focus on those risks that would be truly significant to the institution (based on a scale that you have defined). For any given strategy or process, there are dozens, if not hundreds, of associated risks. Focus on the ones that really matter, but don't ignore all of the other risks. The key risks will flow up into the enterprise assessment, but those non-key (but still meaningful) risks need to be identified, tracked, and managed by the business units. By documenting these more realistic day-to-day type risks, each business unit will increase its awareness and active management of them and make risk management a part of their everyday world. But these minor risks need to be excluded from the enterprise analysis because they would obfuscate the major risks.

Consider whether risks are strategic or operational.
Every institution faces two fundamental types of risk:
1) strategic, macro level risk, such as the business model, products and services, technology, philosophy, human capital, even strategy itself and 2) more micro, operational level risks associated with processes. Macro level risks may have many risk owners, may involve difficult-to-mitigate components (e.g., external factors), and often impact the entire institution, whereas operational risks are typically connected to a specific process with a specific process owner. An effective enterprise risk assessment should be able to consider either type of these risks.

Later on we will discuss two different approaches to risk assessments, one based on risk types and one based more on process. Regardless of which method the institution chooses to use as a basis for its assessment, it's important to understand the role risk types play in evaluating and sizing risk. Simply put, risk is not managed by risk types. There is no such thing as a reputation risk in isolation from other kinds of risk.

Everything banks do introduces other more specific and wide-ranging types of risk. We need to think of risk types as lenses through which we view our organization and by doing so gain a deeper understanding of the nature and scope of risk. But only by considering all types of risk do we really learn how we should manage risk. In other words, if you are thinking about a given process and the risks associated with that process (plausible alternative outcomes), there is great value in saying, "For that failure scenario what is the credit risk? The compliance risk? The reputation risk? The liquidity risk?"

By considering potential risks—strategically or operationally—we learn a little bit more about the impact of that risk, and are better able to make decisions about whether the right level of controls is in place. In this workbook, we describe how institutions conduct specific risk-type assessments. These assessments can be very informative, but they should be used with caution. A risk will be underestimated if the full spectrum of impacts is not considered.

Know the difference between risks and risk sources.
When considering risks to the institution at an operational level, one of the most common trouble spots is confusing risk sources with actual risks. This confusion can make quantifying (sizing) risks extremely difficult because, unlike risks, risk sources cannot be reasonably quantified.

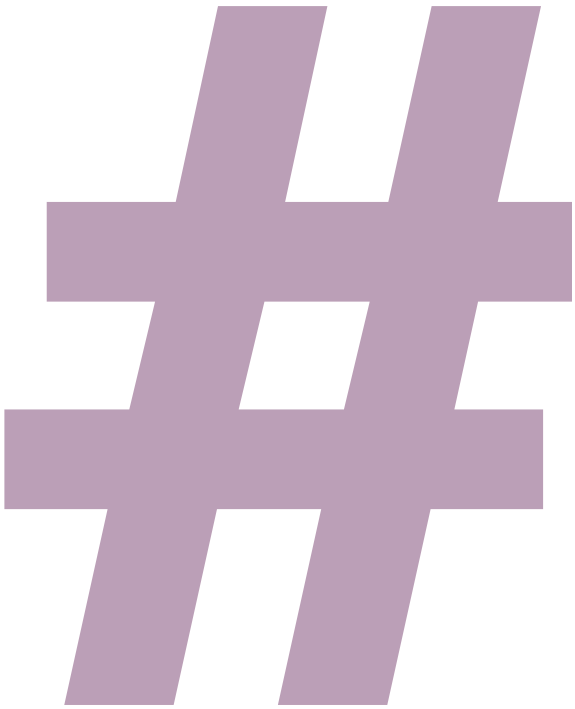
Common examples of key risks include:

- Unauthorized wires due to fraudulent activity.
- Failure to authenticate callers leading to unauthorized account access.
- Failure to complete timely patch management.

In each of these cases, we can quantify the impact of the failure on the institution because we know the outcome to be, for example, financial losses or data compromise.

Common risk sources include:

- Lack of policies or procedure.
- Insufficient staff or staff turnover.
- Lack of sufficient training.



The risk sources are shortcomings that make a process failure more likely, but since they are not a process failure, they are almost impossible to quantify. Put another way, risks are what could happen, and sources provide insight into *how* it could happen.

This distinction is also important because we seek to quantify and assess risks, whereas we generally impose controls on risk sources, such as policies and procedures or sufficiently trained staff. Both points of data are important to assessments but for very different reasons.

Make ERM the hub.
ERM is often described as the hub of risk management, the center to which all other elements should connect. This is especially true of risk assessments. The institution conducts a range of risk assessments, from compliance to information security, BSA to ACH[3]. Each of these specialty assessments are focused on one specific type of risk within the overall universe of risks. These results provide specific information about one type of risk and can offer insight into whether the appropriate level of controls are in place.

3 The automated clearinghouse (ACH) system is a nationwide network through which depository institutions send each other batches of electronic credit and debit transfers.

If an enterprise or operational risk assessment duplicates these assessments, should you ignore them or incorporate them? Best practice suggests that specialty assessments should continue to be conducted because they serve a specific purpose. However, enterprise or operational assessments should be designed to take specialty assessments into consideration and incorporate the results in a meaningful way. For example, the bank conducts an information security (IS) risk assessment that considers the bank's overall IS risk. This assessment can be incorporated into an enterprise or operational risk assessment at a high level as one line item in the strategic part of an ERM risk assessment or it could be incorporated by providing a security risk weight to each business unit. And while the ERM or ORM risk assessment will show a summary score, the narrative should point to the detailed IS risk assessment should the reader want more detail.

Understand that a risk assessment is not just a control assessment.
It is important to realize that the primary purpose of a risk assessment is to carefully evaluate the inherent risks to the bank and each of its operating areas. Oftentimes people develop or use risk assessments that are primarily questionnaire-based (more under Risk Assessment Methodologies below). Those assessments tend to focus more on questions about controls, rather than on the nature of risk itself. As part of an enterprise risk assessment, you absolutely want to evaluate your strength of controls, but only within the context of the level of risk. The goal is not just to determine whether the control is being enforced, which is the job of Internal Audit, the goal is to understand the risk itself, and determine if the control design is adequate to mitigate risk. Questions like "Are separation of duties maintained?" is an audit question, whereas "Do separation of duties exist?" is a more appropriate risk assessment question.

Understand inherent and residual risk.
These concepts are fairly well known and most institutions already incorporate them into their risk assessment structures. In short, inherent risk is the level of risk that exists before any risk treatments are put in place. Conversely, residual risk is the risk that exists despite the risk mitigants in place—what could still go wrong despite the controls. While these concepts are straightforward, there are a few aspects worth noting. Inherent risk is sort of a silly concept, since controls will always be in place. However, understanding inherent risk is critical to any risk assessments because it creates the context for what level of controls should be in place based on the severity of the inherent risk. If you don't size the base risk, you have no idea what level of controls should be developed. Residual risk is then the risk that you chose to accept because the cost of incremental controls would exceed the risk exposure. Residual risk is what is compared against risk appetite levels because it is the risk you accept. The goal for every risk assessment, regardless of what is being assessed, is to determine the residual risk. Understanding your residual risk allows you to answer the question, "Has the risk been reduced to an acceptable level?"

Understand the four ways to treat inherent risk:
1. Avoid the risk by not undertaking the activity or business.
2. Transfer the risk to third parties.
3. Mitigate the risk by creating suitable levels of controls.
4. Accept the risk while acknowledging what could go wrong and build no further controls.

Be aware of emerging risks.
Emerging risks are those risks that are not meaningful to the institution today, but could become so in the foreseeable future. A good enterprise or operational risk assessment should consider emerging risks and document the assumptions about why the risk is a real risk and what parameters should be monitored for changes that could indicate a real and present risk. Often risk assessments are broken into two sections, one that covers known, current risks, and a separate section that discusses emerging risks.

Never, ever start by asking a business unit, "What are your key risks?"
The question is too open-ended for average business staff who are focused almost exclusively on getting their jobs done every day. They often have only a vague idea of what can actually go wrong. To jump from zero to "What are your key risks?" is too big of a jump. Instead, start by asking something that they know. In most cases, that means asking about their business processes and discussing normal, expected outcomes. From there, it's usually a pretty short hop to "What could go wrong?" which is another form of "What are your risks?" The general rule with any risk assessment, regardless of its scope or focus, is "start from what you know that you know." Always give yourself a solid foundation on which to build.

Document assumptions.
Regardless of the method used to assess risk, it is critical to document key assumptions because risk always lies in the assumptions people make about:

- Why they believe the risk is real.
- Why they believe the controls are strong and are being maintained.
- What it would mean if the risk materialized.

Documenting assumptions gives everyone an opportunity to know what people assume and provides a forum to challenge those assumptions.

Set the tone.
Setting the correct tone is critical to the success of any type of assessment. Make sure the business units understand why you are doing the assessment and what you are trying to discover. Be clear that honesty is essential if the assessment is to be truly valuable to the institution. You don't want the business units to waste everyone's time by providing answers that they think are the correct answers. Only when the business units are encouraged to be honest and transparent about risks and control strengths and potential weaknesses will you get the full value from the exercise.

Realize where the assessment value lies.
While reports and graphs and risk scores are all very interesting and make for colorful reports, the real value from a risk assessment comes from the dialog that it creates. Dialog creates awareness and awareness leads to accountability.

IV. RISK ASSESSMENT FOUNDATIONS

When building an enterprise or operational risk assessment, you must determine the focal point of the assessment, also known as the assessment foundation or basis. You then need to determine the approach or level of detail that you need.

A risk assessment can be structured in a variety of ways, but this workbook focuses on the two most common structures, which are based on:

- Risk types.
- Enterprise details, such as strategy and processes.

RISK-TYPE ASSESSMENTS

Risk-type assessments focus on a series of primary risk types (e.g., strategic, credit, liquidity, market, interest rate, operational, reputation, compliance, etc.) examining possible sources of risk. To assess credit risk you would typically review:

- Credit policy.
- Underwriting criteria.
- Credit concentrations.
- Historical portfolio performance.
- Allowance levels.
- Strength of the credit and lending staff.
- Market conditions.
- Potential interest rate changes.

The assessment would involve discussions with various executives, departments, and external subject matter experts, each of which could provide insight into the nature and scope of credit risk in the areas described above. Not every area needs to be involved in this assessment since there are a limited number of areas that represent a source for credit risk.

For other types of risk, different staff would be involved. An operational risk assessment would review areas such as branch operations, deposit operations, loan operations, and IT. (In truth, operational risk exists with every person in the company.) Liquidity and interest rate risk assessments would probably focus more on the finance function and its decisions about setting and managing ongoing liquidity levels and asset/liability compositions. Compliance risk assessment involves an evaluation of the laws and regulations applicable to the institution and as well as the policies, procedures, and training in place to ensure compliance. This assessment is probably already being conducted by the bank's compliance department.

The following is an example of a matrix based on this type of assessment:

Risk Type	Inherent Risk Rating	Risk Mitigation Strength	Residual Risk Rating	Risk Trend
Strategic	Very High	Strong	Low-Mod	→
Credit	Very High	Strong	Low-Mod	↘
Liquidity	High	Satisfactory	Low	→
Market	Moderate	Satisfactory	Low	→
Interest Rate	Moderate	Strong	Low	→
Operational	Very High	Needs Improvement	Moderate	↗
Reputation	High	Satisfactory	Low-Mod	→
Compliance	High	Satisfactory	Moderate	↗

Building a risk assessment using this approach has notable pros and cons.

Pros:

- This approach can be easier to complete since you are only focusing on one risk type at a time, which limits the number of areas you need to address.
- It can lead to meaningful risk assessments (and likely some follow-up action items) much quicker.
- This approach can be done with limited resources, and is, therefore, often a good choice for a small bank.
- For larger institutions that often have defined risk groups dedicated to specific risk types, this approach provides directly meaningful insight into risks within their domain.

Cons:

- This approach can make it difficult to connect risks to specific, individual controls since some risks can manifest in a variety of ways sourced from a number of different places.
- This type of assessment may be more subjective since the bank may not have a lot of related data to build into the analysis.
- By focusing on only one type of risk at a time, certain types of risks may be dramatically underestimated. For example, a given event scenario could represent multiple types of risk which, when added together, represent a substantial risk to the institution.
- Looking at risk in silos increases the chance that risks will be missed because staff viewed a certain risk as "the other guy's risk." Disagreements may arise about a specific risk in trying to classify it into a risk type, which is counterproductive to effective risk management.

DETAILED ASSESSMENTS

If the institution wants a more comprehensive method to assess enterprise risks, it can take a more detailed approach in which the basis, or foundation, becomes macro-level issues such as strategy and governance as well as operational-level processes. With this method, risk types simply become factors in the assessment, giving further insight into the scope and nature of the risk.

For example, at an operational level, a common key risk is unauthorized outgoing wires due to fraud. This risk can be easily quantified since the outcome is clearly defined, based on the different risk types that this event represents:

- *Strategic.* Yes, large enough losses could have strategic implications.
- *Credit.* No, credit risk requires an obligor.
- *Liquidity.* Yes, large enough losses could lead to liquidity issues.
- *Market.* No.
- *Interest rate.* No.
- *Operational.* Yes, this is a notable operational risk with significant impact.
- *Reputation.* Yes.
- *Compliance.* Yes.

By contemplating the collective impact of multiple risk types, we gain a much more detailed and accurate picture of the true scope of the risk in question.

A simple assessment format includes references to specific risk types, again giving the reader a better understanding of the impact of each risk scenario. Building data in this way can also allow the institution to summarize the information to see which risk types are more concentrated. Please note, however, that operational assessments (those based on processes) will largely represent operational, compliance, and reputation risks by their very nature. A strategic/macro level assessment will reflect more strategic, credit, interest rate and market risk since those risks are largely associated with strategic decisions.

The following is an example of a more detailed assessment, identifying individual process risks and considering risk levels, both in terms of inherent and residual risk. It also classifies these risks into the impacted risk types.

						Strategic	Credit	Interest Rate	Liquidity	Operational	Compliance	Price/Market	Reputation
Process	**Risk**	Inherent Risk Rating	Risk Mitigation Strength	Residual Risk Rating	Risk Trend	**Risk Level** (0-None, 5-Very high)							
Wire transfer	Unauthorized wires	Very High	Strong	Moderate	→	3			3	3	2		2
Wire transfer	Inaccurate posting of incoming wires	High	Satisfactory	Low-Mod	↗					2	3		3
Wire transfer	Failure to post wires in a timely basis	Moderate	Satisfactory	Low-Mod	→						2		2

To be successful, this type of assessment needs to be completed at both a strategic (macro) level and an operational (micro) level. At the strategic level, areas of focus could be products and services, physical or geographic locations, strategic initiatives, areas of corporate governance, and so on. These are all strategic, tactical areas of risk that affect the entire institution and are based more on strategic decisions than operational processes. This part of an assessment can also consider external risks, which are largely outside of the institution's control.

The operational side of this type of assessment is much more straightforward; it is based on the individual processes used by the institution to execute its day-to-day operations. These have specific owners, connect directly to operational controls, and provide a concrete foundation for the assessment. (The business line may not be sure about their risks, but they are sure about their processes.)

Again, in each case a risk rating can be applied to every element within the assessment, whether or not you decide to include the individual risk types within the analysis. However, if you include the individual risk types, you will get a much better analysis.

Building a risk assessment using this approach also has notable pros and cons.

Pros:

- Provides much more actionable information.
- Makes it much easier to associate risks to specific controls, since you can identify the specific owners for each process assessed.
- Supports consistency with the Internal Audit process, which is almost always tied to processes and the related internal controls.
- Allows all business units to use the same template structure to identify more routine operational risks as well as to identify key risks.

Cons:

- Takes more time and resources to conduct.
- May be more burdensome on business units since they will likely have to document more information about risks and controls.

V. GENERAL SUGGESTIONS

GENERAL SUGGESTIONS FOR ENHANCING THE ERM PROCESS FOR RISK MEASUREMENT, EVALUATION, AND COMMUNICATION

Although there is no "one size fits all" for implementing this piece of the ERM process, this section is intended to advise community banks and other noncomplex financial institutions. Remember, successful ERM processes must be both customized and adaptive.

To focus management and the board on the most important risks, your institution must have a basic risk appetite and risk metric framework in place. Those are building blocks and critical first steps in raising risk awareness and demystifying ERM. If they are not in place, please refer to the previous RMA workbooks and materials and start from there.

First, a few general suggestions to smooth the ERM path up to, and through, risk measurement, evaluation, and communication:

- *Keep it simple.* Don't overload your constituents with volumes of complex information. Keep it short, tactful, and direct.
- *Repetition can be your friend.* There is value in an ongoing risk focus, awareness, and consistent communication.
- *Know your audiences.* Be flexible in your information and delivery formats. Does your audience prefer data or graphs or both?
- *Be outcomes-based.* Have a clear desired outcome for any action. Working back from there will help you hone the message.
- *Don't recreate the wheel.* You can borrow from plenty of internal and external sources, such as RMA, the American Bankers Association, regulators, vendors, and working groups. Take this opportunity to bring available information together, simplify it, add your perspective, and focus within the established risk framework. Don't repeat or rehash information senior management and the board is already getting.

VI. HOW TO FOCUS ON THE KEY RISKS

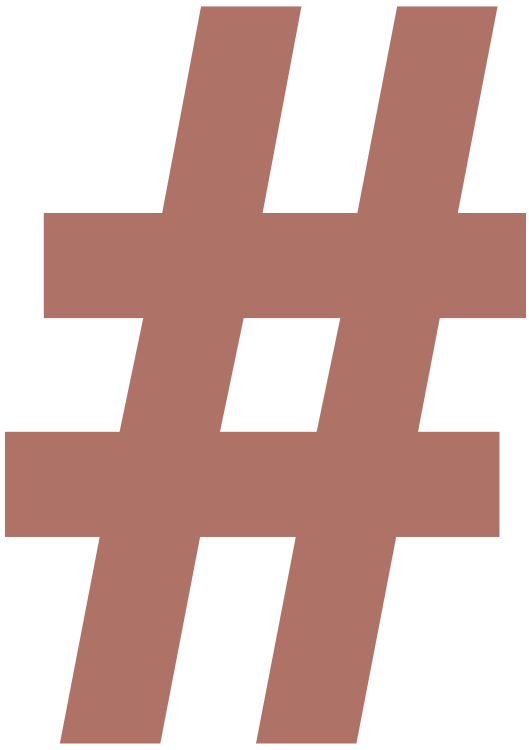
By definition, ERM is an enterprise responsibility. You should not personally or departmentally own risk management. Instead, be a sponsor or foster shared responsibility, drive accountability, and lead by example.

As risk professionals, we know the importance of an independent perspective and the three lines of defense in a control environment—the business unit, internal audit, and risk management. Other sections of this workbook provide guidance on inherent risk identification, residual risk, and the importance of risk sizing. We need to take every opportunity to put the most important risks at the forefront and bake them into the board and management reporting process over time.

Below are four basic steps you can take to draw your organization's focus on the most important risks in a community bank.

STEP 1: INVENTORY THE RISKS

Inventory, bucket, and rate the risks present, including the names of those who are accountable for them as well as the available data points for each risk. Not all risks may be in the framework, but most should be. Determine the frequency of each risk and the collective ability to influence the risks perceived to be the most important. A thorough periodic inventory will help identify gaps and the impact on the risk appetite statement and/or framework. For assistance, please refer to the *RMA Risk Appetite Workbook* and *Section XIII* of this workbook.



STEP 2: PRIORITIZE

Following are some options for grouping, sizing, and adding perspective in the prioritization process. When cataloguing risks, it is better not to use numbers or letters (1, 2, 3; A, B, C). Readers may believe those numbers or letters indicate a priority ranking. If your intent is to create a priority ranking, then the use of letters and numbers is fine. Otherwise, consider using risk grouping, heat mapping, or a less granular listing technique.

Start risk prioritization by focusing on the relatively few risks that can cause a small, noncomplex financial institution to fail or stop it in its regulatory tracks. Relying on our collective prior experience, the list is fairly short:

- Liquidity risk.
- Credit quality.
- Concentrations.
- Interest rate risk.
- BSA[4]/AML[5].
- CRA[6], Fair Lending[7], or UDAAP[8].
- Widespread breach or fraud.
- Other risks specific to your company.

> Generally, for large banks, credit risk is what gets a bank sick, liquidity risk is what kills it.
>
> Generally, for community banks, credit risk is not only what gets a bank sick, but also kills it.

Once you have prioritized the most serious risks to your institution, it may be beneficial to group and simplify an almost infinite number of risk factors that can impact your profile. It is also helpful to divide the risks between those that need attention now and those that are safe in a *monitor* or *watch* mode. This exercise will help you determine if your company is operating within the broad context of its risk appetite statement—in other words, in a safe and sound manner.

Another good practice is to have the business unit do a self-assessment of the priority risks and then have the risk team do the same. The differences in their assessments reflect a healthy, effective challenge process.

Next, you need to decide whether the risk would benefit from current mitigation activities. Examples of current mitigation include reducing concentrations, modifying credit score cutoffs, or adding resources to complex projects. For risks that don't benefit from near-term mitigation but are both present and significant, be sure to note the consequences of inaction and rationale for deferral. Although "doing nothing" (business-as-usual risk) may be best at this time, both action and inaction have consequences. As risk professionals, we recognize that not everything can be, or should be, done at once. This is, after all, an exercise in risk prioritization and focus.

---

4 The Bank Secrecy Act is codified at 31 U.S.C. §§ 5311 et seq.
5 The USA Patriot Act, Pub. L. No. 107-56.
6 The Community Reinvestment Act (CRA), Reg 12 CFR parts 25, 228, 245, and 195.
7 The Fair Housing Act, Title VIII of the Civil Rights Act of 1968, 42 U.S.C. 3601-3619.
8 Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. §§ 5481, 5531, and 5536(a), all covered persons or service providers are legally required to refrain from committing unfair, deceptive, or abusive acts or practices (collectively UDAAPs) in violation of the act.

If times are generally good for your company, business model, or economic environment, make sure there are allowances in your current framework for the possibility of a stressed environment. If the allowances are not clear in terms of metrics, ranges, tolerance, or appetite, allow room for risks susceptible to stress in your prioritization.

There may be risks specific to certain business units or geographic and corporate entities. If it is a stand-alone, specific risk toward the top of the developing priority list, internal accountability should be straightforward. However, if there are multiple departments, geographies, inputs, or variations by unit on the same basic risk, consider grouping them for simplicity of presentation. You can then focus on shared accountability and broader action timelines in the next phases of the ERM program: response and mitigation.

STEP 3: TRANSLATE

This step attempts to find common denominators in identified risks and risk communication strategies. You don't want to lose sight of the banking basics here and underestimate the impact of growth, concentrations, and new lines and products on a risk profile. These should be addressed in your risk framework.

Translation involves converting the work on inventory and prioritization into tangible potential impacts. In other words, make the risk appetite statement come to life with measurable, actionable, and communicable risk metrics, such as the impact on capital/earnings. This is not an overnight process and requires patience, consistency, repetition, and diplomacy. Take every opportunity to tie day-to-day activities, issues, or adverse events to the appetite, framework, and risk prioritization.

Format the formal presentation and communication of risk prioritization according to your audience's preference. Consider the best way to do so simply, and remember that tracking the risks over time will typically be necessary. Is a matrix appropriate? What about heat mapping or combining it with narrative?

Most risks in noncomplex institutions lend themselves well to risk metrics and are simple to quantify. However, risks such as operational, reputational, legal, or strategic are harder to quantify and can be difficult to translate. A short narrative may be the most appropriate way to address those. It should focus on trending as well as internal or external qualitative factors such as press coverage, stock price, or client feedback. In broad terms, capital levels are the primary buffers—as they are for most risks. Attempt to gather data points for the narrative, but absent clear correlations, don't push to recognize hard-to-quantify risks in the metrics framework. Instead, work toward robust metrics and correlations as your company grows in size and/or complexity.

As a dedicated and typically independent risk management resource, you can add value by making sure emerging economic, regulatory, or operational risks are on the table. A sample briefing template for emerging risks can be found in the appendix.

STEP 4: REVIEW

Once you have communicated the most important risks, the final step is a look back. Take the learnings from this round of communication and make the process continuously better. Ask yourself and your internal partners the following questions:

- Is the risk appetite statement still valid?
- Is the framework more informed now?
- Did we identify risks or risk groupings that were not in our inventory?
- Did we get valuable feedback from the decision makers in our company?

Embrace continuous change and revisit the risk appetite, framework, inventory, and communication strategy. Be flexible and adaptable. Discussing revisions to the strategies with your peers will minimize communication missteps with your audiences and bring additional clarity to the enterprise risk profile.

The review will be useful in conversations with executive management and the board and will enable the next steps in the ERM process: response plans and triggers. Further, it solidifies and documents business choices over time and will assist in evaluations of their impacts.

VII. A STRUCTURED APPROACH TO RISK MEASUREMENT

Risk measurement is the cornerstone of effective risk management. Many risk professionals are experienced enough to sense risk and effectively manage it; however, a more structured approach is required in today's complex business environment.

Typically, effective risk measurement that supports factual, objective, consistent, and repeatable risk management undergoes four evolutionary phases:

1. Measurement.
2. Theory building.
3. Risk sizing.
4. Governance.

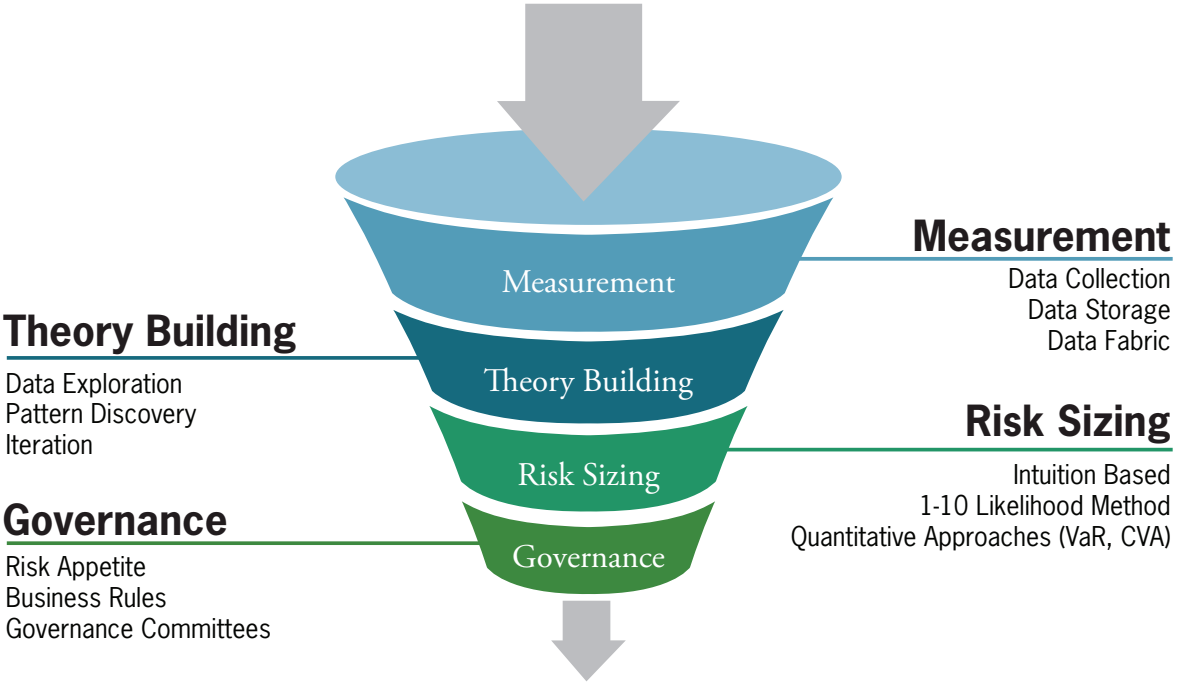


Figure 1: The Risk Measurement Lifecycle

Each of the next four chapters discusses the components of the risk measurement lifecycle.

VIII. RISK MEASUREMENT

DATA COLLECTION

The first component of risk measurement is data collection. Risk data should be gathered from both internal and external sources. Typical internal data sources are back- and front-office systems, legal and compliance, accounting, and trading systems. Some typical external data sources come from business counterparties, regulators, markets, industry groups, and financial utilities or intermediaries.

Regardless of the data source, care must be taken to ensure that different data sets have at least one measure in common, preferably two or three. That way, data sources can be combined with each other, and simple relationships can begin to be uncovered and aggregated.

Whenever possible, risk data should be centrally stored in a consistent manner. The ideal storage solution should be some form of relational database; however, a central repository for spreadsheets and/or raw data files can be effective as well.

With the advent of new data technology, the cost of data storage is at historical lows. As of February 2017, the cost of one terabyte (TB) of storage was less than $75. Because data storage is so cheap, a dangerous trend known as data intoxication is emerging in the business world. Operating under the incorrect assumption that more data is better, businesses are vacuuming up enormous piles of data to the extent that noisy or irrelevant data has become difficult to distinguish from valuable data.

As such, the best practice for data collection is to assume that more data is not always better and that too much data can be detrimental. Risk managers and business leaders should subject new data sources to evaluation, experimentation, and trial periods before adopting them into production spaces, with an emphasis on internal data. The use of external data needs to be justified and/or supported so that it matches or is similar to your bank's data characteristics.

DATA STORAGE

Risk data can be contained and stored in many ways, including in databases, text files, spreadsheets, and business software applications. As a best practice, emphasis should be placed on ensuring that risk data is open and easily accessible to the analytic communities within your enterprise. The more quickly and efficiently risk data can flow through the enterprise to different organizations and decision makers, the more quickly and efficiently the enterprise can actively detect and manage risk.

There is a long-established practice of segregating risk data from other non-risk business data. Although the rationale may be justified and often varies between businesses, the practice of isolating risk data comes at the price of stifling innovation. Whenever appropriate, interconnectivity between risk and non-risk data should be encouraged in order to better empower risk and business analysts to operate at the peak of their abilities.

DATA FABRIC

As previously mentioned, risk data can be combined with other data sets in order to enhance the data or to uncover deeper relationships (e.g., external data). Risk data should be open to risk and business analysts and have appropriate, although not overly restrictive, access permissions. If risk data contains particularly sensitive information—say, social security numbers—the best practice is to partition the data behind some security barrier or to sanitize the sensitive information out of the data set so that it is appropriate for use in a pseudo-public setting.

Take care not to completely isolate a sensitive data set; otherwise, the value of the data is severely diminished, sometimes to the point where security and administrative costs outweigh the intrinsic value of the data itself. Be mindful of the need to comply with the Gramm-Leach-Bliley Act (GLBA)[9] and The Payment Card Industry Data Security Standard (PCI)[10] requirements, which include a framework to protect sensitive consumer data.

The graph is a theoretical map of what a healthy data fabric should look like. Each circle, called a node, represents a unique data repository (risk, operations, AML, etc.). It is called a data fabric since each data node is woven into the other nodes.

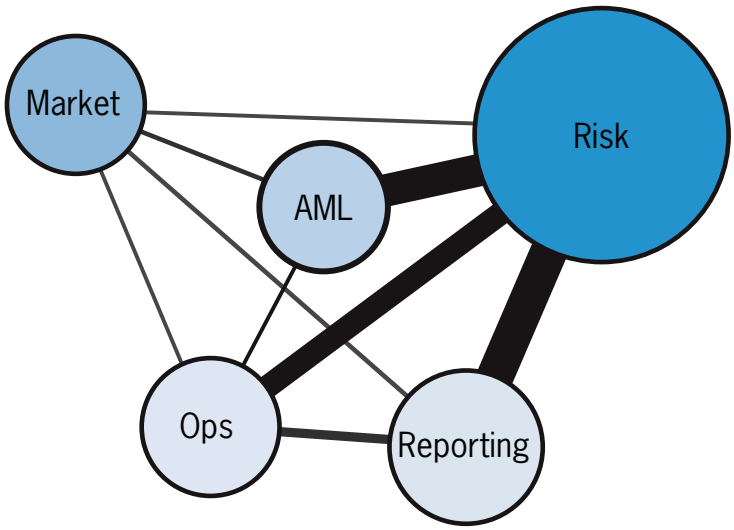


Figure 2: Example of a Healthy Data Fabric

Businesses with effective risk management capabilities are generally those that focus on creating and cultivating data policies that stipulate:

- Data should be open and appropriately accessible to analysts and management.
- Automation should be used to compile data and produce analytics whenever possible.
- Interconnectivity should be encouraged to enhance analysis capabilities.
- More data or analysis is not always better. When you are getting diminishing returns, move on to something else.
- An analyst's time is best spent on reviewing analysis, not on compiling analysis.

9 The Gramm-Leach-Bliley Act, 113 Stat. 1338.

10 The Payment Card Industry Data Security Standard is a set of requirements set forth by the Payment Card Industry Security Standards Council. They are designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

IX. THEORY BUILDING

EXPLORATION

Theory building is the next major building block of an effective risk management program. Theory building is the *iterative* process of attempting to observe and categorize events with the intent to explain the cause of the observed events. By exploring the data, basic relationships are uncovered that can lead to a more comprehensive risk perspective. Below are some common relationships to look for in data:

1. Aggregates: Determining sums, averages, medians, or rolling sums.
2. Frequency: Simple counts of arbitrary events.
3. Changes: Observations on how data changes over time or across business units.
4. Cross references: Investigating common elements between different data sets.
5. Correlation: Measurements to determine interdependence between different data.
6. Dispersion: Measurements to determine the data's volatility or propensity for change.
7. Indicators: Identifying leading and lagging relationships in the data to identify early warning indicators of stress.

There are two main motivations for investigating the above relationships. The primary motivation is to gain insight into the data and learn how the data, which is ultimately a measurement of a business process, ebbs and flows. The second motivation is to raise additional rounds of questions that will drive deeper and deeper analysis. For example, consider the random daily price change of an arbitrary asset. A deeper understanding of the behavior of this price change can be obtained by looking at simple aggregates in the form of minimum, maximum, and mean. Additional insight is gained by measuring the dispersion of price changes, accomplished by measuring the standard deviation. Lastly, a histogram of daily price returns is generated for the entire sample timeframe.

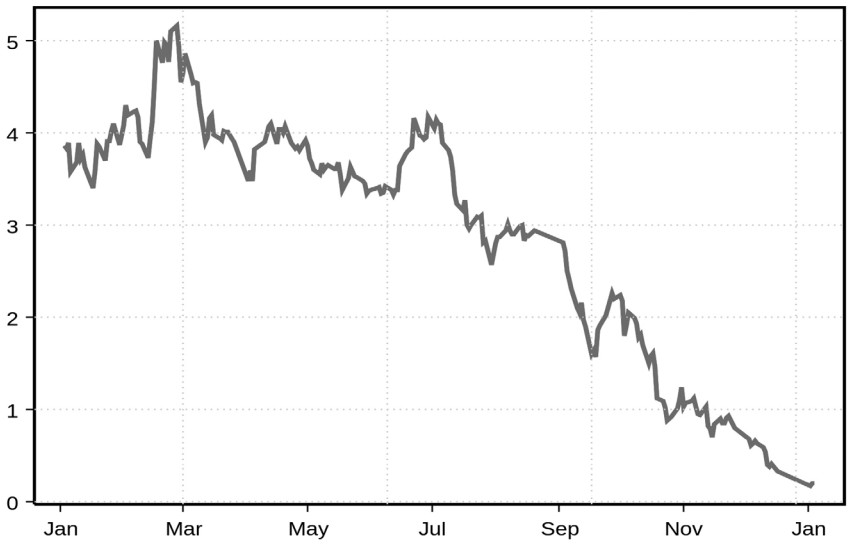


Figure 3: Daily Prices

Measure	Value
Min. Daily Change	0.003%
Max. Daily Change	22.31%
Mean Daily Change	0.34%
ᵒ Daily Change	3.90%
Normal Daily Change	-3.6% | 4.2%

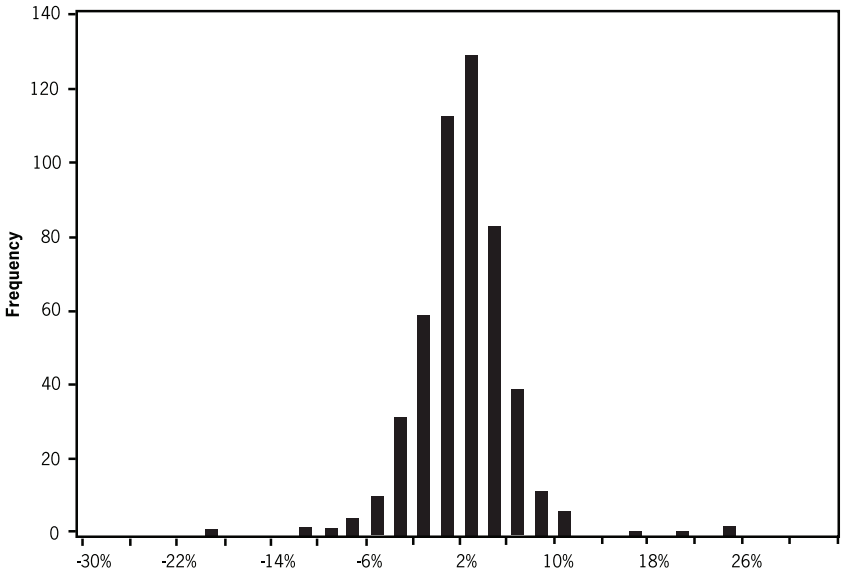


Figure 4: Measurements and Histogram

By combining several simple measurements, we gain a more complete understanding of this asset's price behavior. We can state the following for the sample window:

1. This asset's price changes about 0.34% each day, on average.
2. On a normal day, the daily price change of this asset will be somewhere between -3.6% and +4.2%.
3. On an abnormal day, the largest daily price change was 22.31%.

By allowing us to understand, this information helps us make informed decisions about the asset.

PATTERN DISCOVERY

After a certain period of exploratory analysis, information is accumulated about specific aspects and relationships within the risk data. As these aspects are viewed together in larger and larger contexts, some useful patterns begin to emerge:

1. Trend: Patterns that tend to exist over a given dimension, usually time.
2. Clustering: Patterns that indicate groups of similar things.
3. Function approximation: Patterns between dependent and independent variables.
4. Classification: Patterns that indicate if data fits into a predefined class or group.
5. Migration: Patterns that indicate if the populations of groups are changing.

ITERATION

The presence, or absence, of patterns will lead to valuable questions and conversations between the risk and business groups. These questions will ultimately provide a foundation for a deeper understanding of the risks within a business segment as well as a feedback loop for continuous understanding of the patterns themselves. The better a business unit understands relevant patterns, the better it can govern and mitigate risk.

X. RISK-SIZING METHODS

Once you have established the basis of the assessment as described in Section 3, you will need to decide what level of detail you need and choose one of the three assessment methodologies discussed below. This section provides you with information to help you decide the level of detail suitable for your institution based on the available time, resources, and data. Although you can use an infinite combination of methods to size your risk, this section focuses on three general approaches:

- Intuitive/judgment method.
- Likelihood/impact method.
- Quantitative method.

There is no right or wrong method. Each methodology has distinct pros and cons and can be used regardless of which foundation you choose for the assessment.

INTUITIVE/JUDGMENT METHOD

Intuition-based risk sizing is based on the judgment and experience of management. Typically, this form of risk sizing occurs in environments where data is scarce. It is based on a combination of professional experience and theoretical conjecture. Examples of this type of risk sizing are what-if scenarios, war games, thought experiments, and stress testing.

The outcome of any intuition-based risk sizing is heavily influenced by individual or collective experience, holistic views of the business, the personality types of management (risk seekers versus risk avoiders), and bias from situations or events that have already occurred or are occurring at the time of judgment.

Risk sizing is especially vulnerable to management's tendency to favor frequency over severity. Specifically, there can be a tendency for management to underestimate exposure to low-frequency, high-severity events. This can be troublesome when, in fact, the purpose of risk management is to protect against such exposures.

The most informal and unstructured method for conducting risk assessments is to distribute questionnaires to management and selected staff, asking them to evaluate the level of risk and controls in place within the areas they manage. This method is commonly used by smaller institutions and institutions that want to quickly complete an assessment for the first time with minimal cost and employee disruption.

Critics argue that this method can be misleading at best and dangerous at worst because it is almost impossible to neutralize people's biases, lack of information, and faulty assumptions. Proponents argue, however, that while the analysis may not be precise, it does offer a tremendous value by encouraging managers to think about their key risks and controls and start to evaluate each in risk terms. It also serves as a foundation for more structured, detailed versions, which should be able to build on the more simplistic model, challenging those biases and assumptions.

In this type of assessment, the institution typically would pick a broad base of either risk types or functional areas. For each assessment area, general questions would be asked to prompt the manager to consider different aspects of risk. This type of approach commonly would take one of two forms:

- Direct approach: "What do you consider to be the overall risk level of your business and what are its key risks?"
- Indirect approach: Each area is asked a series of questions. In theory, the answers to those questions provide some insights about the risk level.

When using the direct approach, the business unit is asked to identify what they believe to be the unit's key risks, providing some rationalization for that perspective. They are also asked to discuss the effectiveness of the controls in place to mitigate those risks.

Following is an example of how Loan Operations may respond to the direct approach risk assessment:

- Strategic: Very low, group is not heavily influenced by strategy, nor do its key risks impact strategy.
- Credit: Low to moderate, there are some select scenarios where staff actions could impede loan collectability.
- Liquidity: Very low, the group's actions do not affect liquidity in a meaningful way.
- Market: None, not applicable.
- Interest rate: None, not applicable.
- Operational: Moderate, there are many potential operational risks that could have at least a moderate level of impact.
- Reputation: Low to moderate, some staff actions could impact customers negatively.
- Compliance: Moderate, the group is subject to numerous federal or state regulations.

The prior descriptions are the inherent risk ratings, which would then be combined with an opinion on control strength, leading to a subjective indication of residual risk. Below is how a resulting table might appear:

	Inherent Risk	Control Strength	Residual Risk	Risk Trend
Strategic	Low	Satisfactory	Low	Stable
Credit	Low to Mod	Satisfactory	Low	Stable
Liquidity	Low	Satisfactory	Low	Stable
Market	None	Satisfactory	None	Stable
Interest Rate	None	Satisfactory	None	Stable
Operational	Moderate	Satisfactory	Low to Mod	Rising
Reputation	Low to Mod	Satisfactory	Low	Stable
Compliance	Moderate	Satisfactory	Low to Mod	Stable

Similarly, this method could be used to assess major functions or processes. A series of basic assessment questions might be developed, such as those for the loan boarding process below.

Process: Loan Boarding

These questions focus on the nature of the risk itself (inherent risk):

- How much volume are you currently experiencing?
- How complex are the loan products that are being boarded?
- What are the worst-case consequences of a systemic failure in the boarding process, particularly if unnoticed for an extended period?
- Do boarding staff have access to other customer records, and can they make changes to those records? Would those changes be flagged and/or recorded in an audit trail?

These questions focus on the control strength:

- Do you have documented policies and procedures?
- Are separation of duties enforced?
- Are the staffing levels adequate?
- Are the staff experienced?
- Have you experienced operational failures recently?
- When things have gone wrong, how quickly did you recover and what was the impact?

A resulting table based on an interpretation of the information might appear as follows:

	Inherent Risk	Control Strength	Residual Risk	Risk Trend
Loan Boarding	Moderate	Satisfactory	Low	Stable
Loan Servicing	High	Satisfactory	Low to Mod	Stable
Loan payoff/lien release	Moderate	Needs Improvement	Low to Mod	Rising
Customer Service/Research	Low to Mod	Satisfactory	Low	Stable

If the institution is going to use a questionnaire-based assessment, it is imperative that the assessment includes questions related to the inherent risk, as well as the control strength, similar to the types shown prior. Assessments containing only questions that challenge control levels will never reveal anything about the nature of the risk; they only inform you about your controls. The purpose of a risk assessment is to provide insight into the nature of the risk (the inherent risk) as well as the related control strength. To only focus on the latter is to perform an audit exercise, not an actual assessment, and will make Risk Management appear like "Internal Audit II," which is not how Risk Management should be perceived.

INTUITIVE/JUDGMENT METHOD: INTERPRETING THE RESULTS

Interpreting the results is largely about understanding the answers to the questions, challenging those answers, and deciding if all of management agrees with the concluding risk ratings and believes that the residual values fall in line with established risk appetite levels. This approach offers several advantages:

- It is easier to complete because it does not require data gathering, aggregation, and analysis.
- Just the process of talking with key business areas about key risks will increase awareness and (hopefully) accountability.
- This approach can be done with limited resources, making it a good choice for a small bank or a bank's first assessment where the goal is to establish a baseline.

While management judgment benefits from years of experience in managing risks, the judgment approach has potential downsides that are not easily apparent and can lead to overestimating or, even worse, underestimating risks. The Risk team will need to take bias into account and challenge responses when they believe the respondent is under- or overemphasizing aspects of risk or controls.

As a general rule, most people will underestimate the risk and overestimate the strength of controls. But even this rule has exceptions. Also, this method can be hard to map to data in support of the analysis; supporting materials may be anecdotal at best.

Key challenges to this approach are:

- *Biases:* Biases are existing opinions, perspectives, or viewpoints held by individuals or groups that can affect the way we think, make decisions, and influence others. Biases can affect the judgment method in multiple ways and could lead to overlooking significant risks or mishandling complex risks.

  – *Individual biases:* Depending on the organization, the sizing of risk lies on the shoulders of an individual or a few individuals, which can potentially lead to a skewed perception of a risk. Individuals sizing risk using the judgment method usually rely heavily on their experience, which naturally comes with its own set of biases. If an individual has had too little experience in managing certain risks or if the experience is too specific to one particular area, then significant lapses in risk sizing could result. In addition, individuals using the judgment method may rely on the first solution that comes to mind based on their bias rather than make an effort to understand all possible options.

  – *Group biases:* The collective dynamic of a group of risk managers often varies, depending on individual members and institutions; however, a strong bias voiced by one member could sway other members' opinions as well. Groupthink biases often emerge, as agreeing easily becomes the norm in most groups. Groupthink biases can become so entrenched that very little discourse takes place, and this can be dangerous to an institution. Confirmation bias is another type of bias that can also take hold in institutions. Confirmation bias can occur when management decides to align or conform the sizing of risks to inherent opinions rather than relying on more objective assessments. Management should take precautions not to let groupthink or confirmation biases set in. One way to do this is by engaging in anonymous information gathering or having a knowledgeable, but independent department aggregate the information. You can also include an effective challenge process in the measurement approach and have open dialogue with the risk owners and identified challengers. By building a culture open to challenging opinions and building a platform that allows for healthy debate, you can minimize the effects of group-based biases.

- *Not casting a wide enough net:* When using the intuition or judgment method, management might not cast a wide enough net to capture all risks. The lack of risk management expertise or experience might make it challenging to classify those risks that are difficult to measure and monitor, such risks as reputation risk and strategic risk. To address this concern, compare your risk inventory to others publicly available, or forge an information-sharing arrangement with an institution of similar size. Comparing the types of risks that a similar institution has identified and is measuring can be an informative exercise and give you confidence that your approach has captured all risks.

- *Too internally focused:* Focusing too many efforts on viewing risks internally is another potential weakness of the intuition or judgment method. External risks from the environment, such as economic, regulatory, customer, and technological, also pose a danger and need to be considered. Be certain that you have an approach for viewing every significant risk you face from both its internal and external drivers. This can address the risk of not considering the outside world and its impacts on your institution.

- *Hubris:* Excessive self-confidence by management could lead to overlooked risks and overconfidence in existing risk management processes. Overconfidence is one of the most common ways to lose sight of important risks. It is also possible to lose focus in terms of evaluating the complexity and size of risks. Be on alert for claims of "That will never happen to us!" or "We don't have any of those types of loans, so we can't be exposed to that risk." While these may be true statements, they bear scrutiny and challenge from independent risk management.

- *Failing to see the "important" trees:* Management's failure to see key risks that could impact the success of the business could have severe consequences. This method has some distinct benefits, especially when sizing risks that are harder to measure; however, it is important to understand the weaknesses. When relying heavily or exclusively on a judgment measurement approach, you should clearly document all of your assumptions and have them challenged by an independent party. Doing so will help minimize the likelihood of missing something significant.

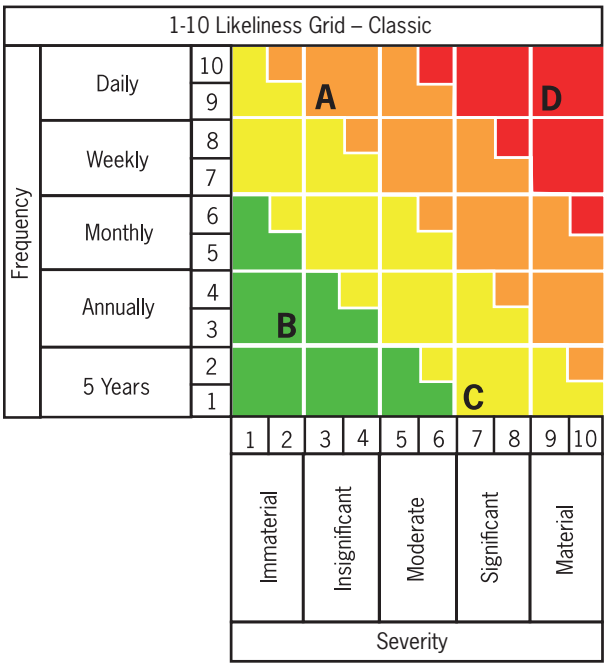
THE LIKELIHOOD/IMPACT METHOD

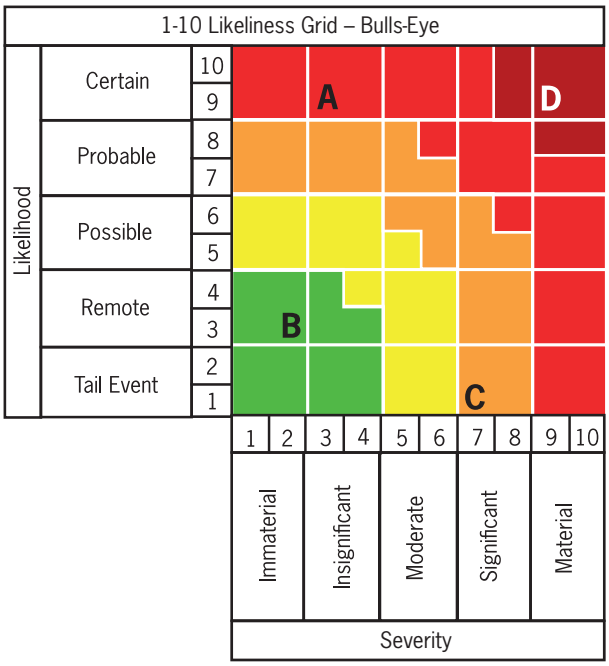
The likelihood and impact method, sometimes called the 1-10 likelihood method, is a form of risk sizing that attempts to quantify different risks on the same scale. This method factors out some of the subjectivity of intuition-based risk sizing and, although it works well in environments where data is plentiful, it also can be used in environments where data is sparse. This method can be a useful tool for a risk manager when identifying and diagnosing risks associated with business units.

The outcome of risk sizing with this method is influenced by empirical evidence, derived during theory building. Theoretical hypothesis are based on a holistic view of the business, individual or collective experience, and bias from situations or events that have already occurred or are occurring at the time of judgment.

Under this method, risks are plotted on a two-dimensional grid with axes that range from one to ten. The Y-axis is used to capture the frequency, or likeliness, of a risk occurring and the X-axis captures the severity, or magnitude, if the risk were to occur.

Color-coded risk severity bands assist with risk ranking and are drawn on the matrix in either the classic diagonal stripe pattern or a modified "top-right of the bull's-eye" pattern.





To populate the matrix, two questions need to be answered: 1) How often does a certain risk event occur? 2) How bad would it be if that risk event happened?

Four examples of risks (A, B, C, D) are illustrated in the examples prior. On first look, risk D in the red band [Frequency = Daily and Severity = Material] seems to be the first risk to address. However, a risk in this region is a strong indicator that the risk measurement process failed, since it is impossible for a risk whose severity is rated material to occur daily and for the organization to still be in business. Therefore, it is logical to assume that there should never be any risk in the top-right red zone. This assumption gives rise to the bull's-eye pattern where the extreme top right turns into the "darker than dark red" zone of disbelief.

A more realistic picture of risk can be seen with risks A, B, and C. Risk A is an insignificant risk, but it occurs daily. Since high-frequency, immaterial risks over long periods of time can add up to substantial exposure and/or losses, they need to be addressed. Risk B is a low-frequency, immaterial risk that can either be a low priority to mitigate or be considered a cost of doing business. Lastly, although risk C is a low-frequency risk, it is a significant risk that can cripple business segments and/or the enterprise.

These low-frequency, material risks are tail events or black swan events and need to be the risk manager's highest priority. They must be adequately understood in order to be mitigated.

The likelihood and impact method is by far the most common method for conducting risk assessments, particularly for institutions in mid-stage programs. It is arguably still only semi-accurate, but in most cases it is reasonable enough, and can often be accomplished with resources available to most institutions. This type of assessment uses interviews or questionnaires and asks business areas to rate their risks based on some notional scale (e.g., high, moderate, low), typically on a three-, five- or ten-point scale. The institution often provides approximate parameters for those ratings.

For a given risk, say fraudulent wire transfers, the institution asks the assessor to assign a risk score to the inherent risk. The score could be calculated as a rating for overall inherent risk or it could be calculated as a combination of inherent likelihood and impact. This more commonly used scoring method is justified with factual, experiential, or referential information.

Likelihood/Impact Structure

For likelihood on a five-point assessment scale, a common hierarchy may be:

Rating	Definition
Very High	A 90% chance of occurring in the next X months
High	A 75% chance of occurring in the next X months
Moderate	A 50% chance of occurring in the next X months
Low	A 25% chance of occurring in the next X months
Very Low	A 10% chance of occurring in the next X months

Another common version is:

Rating	Definition
Very High	Event would likely occur weekly
High	Event would likely occur monthly
Moderate	Event would likely occur annually
Low	Event would likely occur once every five years
Very Low	Event Would likely occur once every ten years

Again, when considering inherent likelihood, you have to assume no level of controls, which can be extremely difficult for some individuals to do. Some argue that considering inherent likelihood is meaningless since it represents an impossible scenario. However, it is important to consider inherent likelihood because it provides the context for the level of controls you should have in place. Nonetheless, assessors should not spend too much time investing in inherent likelihood since there is no level of controls for those events, most of which are a virtual certainty. Inherent impact is much more informative in understanding inherent risk.

There are a variety of ways to establish an impact rating. Generally speaking, the easiest way to consider potential impact to the institution is to evaluate the effect on capital (financial losses), reputation, and regulatory impact, although an almost infinite number of parameters could be used. These three parameters alone can usually provide enough information to fully understand the potential impact of an event, although many others can be added. Regardless of which factors are used, it is important to give assessors some definition around potential impact because this is arguably the most important factor in sizing risks effectively.

Using a similar five-point assessment scale for impact, a common hierarchy may be:

Impact			
Rating	Financial	Reputation	Regulatory
Very High	Greater than a $10mm loss	Extensive media coverage with a significant customer complaint.	Significant regulatory criticism leading to fines and sanctions.
High	Greater than a $1mm loss	Notable media coverage with modest customer complaints.	Regulatory criticism leading to orders and/or MRAs.
Moderate	Greater than a $200k loss	Limited media coverage, small number of customer complaints.	Regulatory criticism leading to MRAs or recommendations.
Low	Greater then a $50k loss	No media coverage and a small number of customer complaints.	Regulatory comments leading to recommendations.
Very Low	Less than a $50k loss	No media coverage and very few customer complaints.	Minimal Regulatory comments or criticisms.

Based on a combination of the inherent likelihood and impact, an inherent risk rating is determined. The following table is one possible technique to determine overall inherent risk, although there are many interpretations about how to establish overall risk ratings.

	Impact				
Likelihood	Very Low	Low	Moderate	High	Very High
Very High	Moderate	Moderate	High	High	Very High
High	Moderate	Moderate	Moderate	High	High
Moderate	Low	Moderate	Moderate	Moderate	High
Low	Low	Low	Moderate	Moderate	Moderate
Very Low	Very Low	Low	Low	Moderate	Moderate

Again, when using the intuitive/judgment method, these values are largely based on the instincts of the individuals being interviewed, possibly supported by related assessments, historical experience, or other reference material.

There are different schools of thought about how closely these ratings should be defined the first time an institution completes an assessment. However, providing quantified parameters to each score ensures that business units will use the ratings in similar ways. The downside is that business units may end up spending a lot of time debating the impact values. Therefore, it may be easier initially to let the businesses decide for themselves what risks are high or low and then fine-tune their responses once you have one completed baseline assessment. Both approaches have benefits and challenges. The question is: Do you want it fast, or do you want it right?

Once an inherent risk rating has been established, the assessor needs to assign a risk rating to what he or she believes is the degree to which the risk has been mitigated, either through transferring some of the risk (through insurance, third parties, or other transfer mechanism) or mitigating it through internal controls (risk treatment). The most common scale for rating risk treatment is:

1. Strong.
2. Satisfactory.
3. Needs improvement.

This three-point scales is the scale most commonly used by auditors and regulators, and it can work well for risk assessments. However, in most cases a five-point scale works better because individuals completing the assessment often find themselves falling somewhere between ratings in the three-point scale. A five-point version could be:

1. World class.
2. Strong.
3. Satisfactory.
4. Needs improvement.
5. Weak.

Each institution will need to decide for themselves what terminology makes sense for their purposes.

Once a risk treatment score has been determined, a residual score is calculated by reducing the inherent scores accordingly. The inherent risk scores could be reduced by using a subjective selection or by applying rudimentary math to determine residual risk. The following represents a simplistic, commonly used method for determining risk scores.

Assuming a five-point scale for each of the rating values (inherent risk, inherent likelihood, and risk treatment), assign a numeric value from 1 to 5 for each rating. To determine inherent risk, multiply the inherent likelihood by the inherent impact. Then, reduce that number by a certain percentage[11] based on the risk treatment rating as follows:

Rating	Risk Reduction
World class	95%
Strong	80%
Satisfactory	70%
Needs Improvement	40%
Weak	20%

11 Note that these values are illustrative and do not necessarily represent standard practices.

So, for a risk that is determined to be high likelihood, moderate impact, and strong risk treatment, the math would work as follows:

Likelihood (4) x Impact (3) = 12, less 80% = 2.4.

From a residual risk perspective, this would represent a fairly low risk. Using this math, a sample residual risk table might look like this:

Residual Risk Rating	Risk Reduction
Very High	> 20
High	> 14
Moderate	> 9
Low	> 3
Very Low	< 3

In the above example, residual risk is calculated. The assessor may want to determine a residual value for both impact and likelihood, which can also be valuable to consider. However, if the assessment is going to calculate a value for residual impact and likelihood, the data that is captured must include additional definitions around the types of controls that are in place.

Controls can be labeled in one of three ways: preventative, detective, or recovery[12]. Depending on the nature of the controls in place, impact and likelihood are affected in different ways, and these variables must be factored into the math calculations. Preventative controls generally reduce likelihood; recovery controls only reduce the impact; and detective controls mitigate both. If the assessment is structured in such a way that control types are documented, this distinction could be factored into the residual risk calculations.

Control Type	Effect on Likelihood	Effect on Impact
Preventative	High	Low
Detective	Moderate	Moderate
Recovery	None	High

There are an almost infinite number of variations on the math that can be used to calculate each of these ratings, but the structure shown here provides a sound, basic framework for a risk-rating calculation. Any model that is developed by the institution to calculate ratings should be documented and tested by an independent party.

12 Auditors commonly label controls as preventative or detective. However, Risk Management should also consider recovery elements, such as training or procedures to respond to an event if it does happen because the faster and more effectively an institution can respond to an event, the further they may mitigate the risk.

The following is an example of this type of analysis, using a 100-point inherent risk scale, based on an analysis of one process area.

Process	Risk	Inherent Risk Likelihood	Inherent Risk Impact	Inherent Risk Rating	Inherent Risk Score	Risk Mitigation Strength	Residual Risk Rating	Residual Risk Score	Risk Trend
Wire transfer	Unauthorized wires	High	Very High	Very High	80.0	High	Moderate	32.0	→
Wire transfer	Inaccurate posting of incoming wires	Very High	Moderate	High	60.0	High	Low	24.0	↗
Wire transfer	Failure to post wires in a timely basis	Moderate	Moderate	Moderate	36.0	High	Low	14.4	→

Some institutions have added *risk weightings* to their assessment tables, giving the assessor the ability to weight certain risks higher than others. This is an ill-advised practice because it introduces another unnecessary subjective dimension. This type of assessment already contains risk weightings by virtue of the level of impact and likelihood. Simply put, higher risks should have higher impacts and likelihood scores; lowers risk should have lower scores. Risk weightings only complicate this process, and provide an unnecessary means for people to game the results rather than to truly think through the risks. It is important to provide guidance to assessors regarding what constitutes high, medium, and low. The same logic applies to control weightings. Controls should be evaluated based on the control strength. Weighting them only muddies the analysis.

Likelihood/Impact Method: Interpreting the results

Interpreting the results for the likelihood/impact type of assessment involves evaluating the assumptions and justifications about inherent risk, risk mitigation, residual risk, and risk trend, and providing challenge to those assumptions. As with the intuitive method described above, consideration is also given to residual risk levels and whether those levels fall within acceptable tolerance levels. Done correctly and comprehensively, the resulting ratings can be compared to the institution's risk appetite statements to determine if the risk levels are acceptable. Because this method is somewhat subjective, the institution should approach the first generation assessment with the knowledge that the resulting analysis will not be perfect, but it will be improved and strengthened with each iteration.

The likelihood and impact method assesses the likelihood of a risk occurring as opposed to assessing the potential impact from the risk event. The method is easy to implement, and all levels within an institution should have no trouble understanding it. Its approach is more structured than the pure intuition or judgment method, and it offers several advantages:

- It forces people to think more thoroughly about the likelihood and impact of risks, and to control strength, resulting in higher accuracy.
- Assessment calculations make it possible to rank risks by their highest inherent and residual risks to determine a more accurate *top risk list.*
- Risk Management and Audit can challenge assumptions about risk and controls and risk ratings because assumptions are more thoroughly documented.

The likelihood and impact method attempts to create structure and root out biases around the sizing of risk; however, it does have certain weaknesses that should be considered:

- *Inexperienced assessment:* Implementation of this approach can be time and labor intensive for both independent risk management and the business lines. When implemented across multiple areas of an institution, this method could strain resources, thereby impacting the quality of the assessments. It is also important to have engagement from the business line at multiple levels of management. Staff-level employees often overestimate the likelihood and/or impact. These assessments need to be determined collectively by a group with the experience to know what the most appropriate scoring might be.
- *Look-alike risks:* Risks can often overlap with other similar risks yet have unique differences. Scoring of these risks with the likelihood and impact method might not reflect the subtle differences between risks. Risks may be scored similarly, but the unique characteristics of each may be lost in the results.
- *Overreliance on the sizing of "important" trees:* Key risks can be identified with a likelihood and impact methodology, but management should not rely too heavily on the accuracy of results from scoring risks.
- *Overreliance on the numbers:* The likelihood and impact method depends on the scoring of risks to express and highlight the significant ones. An overreliance on the scoring, however, could be detrimental if faith is placed exclusively in these numbers. Layering judgment over the scoring methodology is recommended since scoring alone cannot capture judgmental factors.
  - *Accuracy of numbers:* Management should view the scored numbers as indicators of risk levels rather than as precise measures. It must be careful not to base decisions solely on the accuracy of the emerging numbers.
  - *Results from addition/multiplication:* Basing management decisions on numbers that are added or multiplied together could result in a distorted view of the risk level. Generally, risk scores are not directly comparable. Aggregating them can lead to grossly overstated risks that waste the bank resources as it addresses them. Or aggregation could cause an organization to severely underestimate its risks and result in a direct loss for the institution.
  - *Correlations:* Correlations are connections or mutual relationships between risk factors that can affect the complexity and sizing of risks. Identifying correlations can be challenging, and incorporating them into a likelihood and impact methodology can be even more so. The individual risks scored through the likelihood and impact method are stand-alone, and management needs to consider their potential impacts separately from the correlations.

Viewing risks through the lens of a likelihood and impact methodology offers the ability to ring-fence difficult-to-measure risks like reputation and strategic risks. It is fairly subjective, however, and subject to the biases of the individuals providing input. The Risk team will need to take bias into account and challenge responses when they feel the respondent is under or overemphasizing aspects. Also, be aware that this method takes more time and requires more resources, often depending on supplemental resources offered by consultants or other third parties.

QUANTITATIVE METHOD

Finally, assessments can be heavily based on quantitative data. Quantitative methods are advanced mathematical modeling techniques that assign expected values to risks. This form of risk sizing can be accomplished only in data-rich environments, and it should not be attempted with poor or inadequate data sets. The subjectivity of these models exists only in the underlying modeling assumptions.

The outcome of this form of risk sizing is influenced by empirical evidence derived from theory building, statistical and financial mathematics, instrument and portfolio-level views of the business, technical skill of the modeling and analytic staff, and management's appetite for executing risk mitigation efforts based on outputs from complex mathematical models.

Two examples of quantitative risk measurement methods commonly found in banking are Value at Risk (VaR) models and Credit Value Adjustment (CVA) models. Quantitative risk measurement is not limited to VaR and CVA frameworks; there are many modeling techniques to choose from.

This discussion of quantitative methods is only a primer; a full treatment of quantitative analysis would be too lengthy and technical for this workbook. Our aim is to provide you with insights into areas where the institution might consider enhancing or expanding its risk assessment framework and process based on more concrete historical data.

Loss data. Several types of data are typically used for quantitative risk analysis, both structured and unstructured. The most common is loss data—results of actual losses attributable to an unexpected event. The fact that a loss occurred indicates that either a control failed or was inadequate or that the institution had not contemplated certain ways a risk could manifest. Either way, this information can provide extremely valuable lessons and insight into future risks. Most institutions don't have a database of sufficient loss information to be statistically meaningful to an assessment, but this information can be supplemented with sample loss data purchased from various sources and filtered for institutions of similar size and composition.

Proponents of loss (and other experiential data) argue that loss data is the only true way to develop accurate and meaningful risk assessments. Critics will argue that only certain types of loss data are correlated in any meaningful way to future events and could cause more harm than good by misleading management about future risk profiles. In fact, both statements are true, so building assessments around loss data should be done only by institutions with the technical, financial, and operational resources to properly source, vet, analyze, and interpret the data associated with using loss information.

Scenario data. Another common source of information is scenario data in which multiple scenarios are developed for various operational events. Each scenario uses various alternatives to key assumptions and parameters. Although scenario data is just an expanded and enhanced version of the single dimension likelihood/impact model discussed prior, it provides much risk insight into possible risk paths based on a range of assumptions.

The quantitative method offers several strong advantages:

- If the data used is accurate, comprehensive, and applicable to the institution, the resulting risk assessments should be significantly more accurate and defensible.
- Good assessment data is often a powerful tool to help people see past their natural biases.
- Assessments based on objective data can often be mapped to a mechanism (key risk indicators) that monitors the underlying data for changes that could indicate a changing risk profile.

Despite these advantages, the use of quantitative models also present challenges, including translating the information in the models into a language that can be easily understood at all levels within an institution. Also the substantial amount of data required for this method is rarely available to most institutions. Assessors also need to be aware that some data are more meaningful than others in forecasting risk profiles, and data sources must be carefully evaluated to determine relevancy and correlation to risks.

When management is reexamining the use of quantitative methods to size risks, it must recognize the limitations of this method by not:

- *Placing too much value on the numbers:* Institutions that have relied too heavily on the outputs of quantitative models without understanding their assumptions and limitations are often caught off guard when risks manifest themselves.
  - *Limits to quantitative models:* Asymmetrical risks or risks with large tail events tends to be harder to capture effectively using statistical modeling methods. Management needs to understand the limits to which risks are captured and how accurately they may be captured; otherwise, a statistical method could lead to a false sense of security.
  - *Arguing about the numbers instead of the risks:* In general, a lot of resources and time go into maintaining and validating models. Having robust and efficient processes in place is crucial, given that valuable resources can all too easily be spent on arguing about the numbers instead of ensuring that risks are adequately captured.
- *Misinterpreting results:* The quantitative results are often not well understood by non-risk managers, and the right interpretation of the results is sometimes lost during aggregation or reporting. If you are building a risk framework heavily reliant on models and quantitative approaches, having skilled risk managers with the ability to translate the results, assumptions, and limitations for non-risk managers is absolutely essential.
- *Losing the forest:* Despite the many benefits of quantitative methods, their narrow scope may not provide the overall picture. To overcome this weakness, you need to have risk managers who understand the limitations of these models as well as the ability to explain them to upper management.

This method is expensive and time consuming. It requires special expertise, and it creates a real risk that people get so lost in the data they lose sight of the real purpose of the exercise, which is to think about their risks and how they manage them.

FINAL NOTE ON THE THREE METHODOLOGIES

When setting up or reexamining risk processes, you must understand the weaknesses associated with risk identification and risk measurement. One approach is not necessarily better than another. You need a good mix of the three approaches that is commensurate with the complexity of your institution's risks. You also must be flexible enough to change the mix as risks change.

The independent risk management function provides two key values: it balances quantitative, qualitative, and judgmental measurement approaches to discern the key risks for an institution, and it proposes risk mitigants to control these risks. Management must constantly refine the processes. Knowing what to do when risk sizing goes wrong, provides management with more information to improve best practices.

XI. GOVERNANCE

RISK APPETITE/STRATEGIES

Risk appetite is the amount and type of risk that an organization is willing to take in order to meet its objectives. Clearly defined and well-understood statements of risk appetite create value by bringing risk management into focus. Risk appetite should serve as the basis for all risk governance decisions and actions.

A well-defined statement of risk appetite should:

1. Reflect the business strategy.
2. Be adequately documented.
3. Have executive and/or board approval.
4. Take capabilities and resources into account.
5. Include quantifiable tolerances for loss.
6. Enable capacity to take on risk.
7. Require periodic review and calibration by an appropriate risk governance body.
8. Be linked to capital and financial planning processes.

Because the process of risk sizing directly supports factual, objective, consistent, and repeatable risk management, risk sizing also supports the definition and ongoing calibration of risk appetite.

BUSINESS RULES

Risk-based business rules are meant to act as front-line tactical risk mitigation tools. Business rules stem from the risk appetite and are based on observations made during theory building. Any hierarchical design of business rules should be based on the results of the risk-sizing process.

GOVERNANCE COMMITTEES

It is a best practice for Risk Governance Committees to be comprised of stakeholders from the business units as well as the risk area. The role of the Risk Governance Committee is to:

- Charter the risk appetite.
- Review the overall risk profile of the firm or relevant business unit.
- Establish and maintain control infrastructure around risk-based business rules.
- Obtain assurances that principal risks are properly identified and managed.

Risk measurement is a process that involves iterative learning and continuous improvement. The information learned through a risk measurement process shapes and feeds the process of risk governance. Properly informed risk governance bodies are capable of crafting effective statements of risk appetite. Through the definition of risk appetite, business units are equipped with the power to employ risk-based business rules as a part of their risk mitigation strategy. This allows for risk to be managed in a factual, objective, consistent, and repeatable way.

XII. METRICS

In the process of delivering products and services to clients and prospects, financial services firms incur credit, liquidity, market, compliance, and operational risk. All of these risks must be identified and managed by limit structures that ensure that the risks taken stay within tolerances established as part of the firm's risk appetite framework. The objective of financial institutions is not to eliminate risks, but to manage those risks and generate a fair return for the risks the institution has elected to take. The purpose of a defined risk framework is to articulate the firm's risk tolerances and to monitor and control those risk exposures against established limits. The framework should define and manage individual and aggregate risks so that the firm does not exceed the established risk appetite. A risk appetite framework should include at least the following key components.

STATEMENT OF THE STAKEHOLDERS' RISK OBJECTIVES

A statement of the stakeholders' risk objectives should be developed jointly by executive management and the board of directors. In some cases, this job may be delegated to the risk and/or capital committee of the board. The statement should establish an appropriate level of risk for the firm and the overall return on capital that is acceptable for the level of risk taken. Often, institutions choose moderate as an acceptable level of risk and a return on capital that is consistent with peer group performance. The level of risk taken can be defined as a percentage of the firm's total economic capital or the percentage above the policy limits set in its base, adverse, and severely adverse forecasts.

MEASURES AND/OR METRICS TO ESTABLISH AND MEASURE RISK TOLERANCES

Once the risk objectives are determined, a framework for measuring risk must be developed. The framework should use metrics to measure performance against the level of acceptable risk. Metrics can include key asset quality metrics, such as criticized, classified, and non-performing loans. Categories of loans should also be measured to avoid concentrations. Category limits can be expressed as total loans of a particular industry or collateral type, or as a percentage of tier 1 capital or economic capital.

Noncredit risk should also be measured. In the case of operational risk, for example, measurements can be expressed in terms of days of revenue in a particular business line or days of expense in a functional unit. Interest rate sensitivity and value-at-risk measurements can be used for market risk. Other corporate-level metrics should be used to monitor the firm's overall liquidity and capital adequacy.

LIMITS STRUCTURES

Metrics used for measurement should be reported regularly and monitored in a limits framework to ensure that limits are not breached. Escalation procedures should be documented, calling for management action plans as limits are approached. Triggers could be used as speed bumps to indicate a near break of a limit—an early warning that requires a portfolio review. The limits that can also be thought of as risk tolerances should be measured at three levels. The highest-level tolerances are at the corporate level and would include measures of earnings, capital, and liquidity. Corporate-level tolerances should be approved by the board, or a committee of the board, and regular reporting should occur at that level as well. Tolerances at the next level down are those that represent the various risk disciplines, including credit, operational, and market risk. These limits would typically be established by executive leadership of the risk discipline. The third level of risk tolerances occurs in the businesses. Business tolerances are used to measure the effectiveness of the business and therefore include key performance indicators in addition to risk metrics. These measurements are approved by executive leadership and/or business risk committees.

MANAGEMENT DISCIPLINES

Management disciplines include the frameworks, policies, standards, and procedures through which corporate risk discipline and business tolerances are communicated, executed, and monitored. Reporting should occur in the first line of defense in business risk committees, the second line of defense in enterprise-level committees, and then finally in the appropriate board committees. It is important to document policies and procedures for establishing and approving tolerances and the escalation of limits breaches. When establishing this framework, consider:

- A well-conceived risk appetite statement contains both primary and supplemental risk measures that form the foundation of the risk measurement inventory.
- The risk appetite statement defines and controls individual and aggregate risks and the means to avoid such risks by not exceeding established tolerances. The statement should refer to policies and procedures that include an escalation process as risk measurements approach limits. The escalation procedure should require management action plans for mitigation and name the authorities for approving action plans and any adjustments to limits. The risk appetite and framework should be approved by internal risk management and committees, if appropriate, and by the board's risk committee.
- The basic structure of a risk appetite framework may include the following five elements:
  - Stakeholder objectives.
  - Corporate risk tolerances.
  - Risk discipline tolerances.
  - Business tolerances.
  - Management disciplines.
- Stakeholder objectives should be developed jointly by internal risk management individuals or committees and the board.
- Corporate tolerances are the high-level measurements of corporate risk, such as earnings and regulatory capital.
- Risk discipline tolerances are those established for the various risk disciplines like credit, operational, compliance, and market risk. Those should be defined in overall enterprise-level risk policies. Tolerances can be expressed as a percent of tier 1 capital and/or as a factor of days of revenue in the businesses or days of expense in the functions.
- Management disciplines represent the body of policies, standards, and procedures through which the tolerances are articulated.
- This initial inventory is supplemented with additional risk measures as required to complete risk reporting, both internal and that which is required by regulators.
- For noncomplex banks, many of the measures included in the inventory are already calculated and reported through the bank's governance systems (e.g., board reporting, Asset/Liability Committee, etc.). As bank size or sophistication of product offerings increases, additional metrics are required to properly size and manage attendant risks.
- Other ways to measure risks include such metrics as risk-adjusted return on capital, earnings at risk, and expected loss.
- The risk appetite statement is a written document that defines the aggregate level and types of risks a firm is willing to accept in order to execute its business strategies. The enterprise risk appetite statement is supported by qualitative descriptions and quantitative measures.
- Guiding principles shape the risk appetite statement into more granular components by risk categories (credit, market, operational) and serve to guide risk-taking activities.
- Metrics are identified to monitor risk-taking activities and should be a blend of spot and forward-looking measures with defined limits. These metrics are cascaded into the lines of business, where appropriate.
- The risk appetite statement, guiding principles, and metrics are defined and approved by the appropriate governing committee.
- Metrics are monitored at least quarterly through risk reporting. Any breaches are escalated and resolved as appropriate.

XIII. SAMPLE METRICS INVENTORY

A robust risk appetite statement includes several risk objective statements for each risk taken in pursuit of a business strategy. It will typically include both qualitative and quantitative statements and metrics covering most, if not all, of the following risks:

- Strategic alignment.
- Earnings and earnings volatility.
- Capital.
- Liquidity.
- Credit.
- Market.
- Operational.
- Reputation, compliance, and legal.
- Diversification and concentration.
- People and compensation.
- Sustainability.
- Other risks pertinent to the institution.

The initial set of baseline risk metrics will then be supplemented with additional risk metrics used for stress testing, including those covering internal data such as earnings, capital, liquidity, default rate, loss given default, commitment, current balance, maturity, demographics, and loan type, as well as external data such as macroeconomic factors, industry benchmarks, and peer data.

Below is an example of a risk metrics inventory:

Capital:

- Regulatory capital (under base and stress scenarios).
- Minimum core tier-1 capital (under base and stress scenarios).
- Regulatory capital buffer (core tier 1, tier 1, leverage, and total).
- RWA limits across businesses (if applicable).
- Largest economic capital exposures to any single name.
- Economic capital allocation by business line.
- External rating by S&P, Fitch, etc. (if publicly traded).
- Optimized capital usage pursued using risk adjusted return on capital (RAROC) and economic profit across the company.
- Leverage ratio minimum %.
- Debt to equity maximum %.
- Double leverage ratio maximum %.
- Dividend payout ratio.
- Achieve satisfactory CAMELS rating for capital adequacy.
- Maintain total equity / total assets within acceptable limits (%).
- Maintain capital ratios above regulatory capital requirements.
- Tier 1 leverage ratio.
- Tier 1 risk-based capital ratio.
- Tier 1 leverage ratio in a severe adverse scenario.
- Tier 1 capital ratio.
- Risk-based capital ratio.

Credit:

- Absolute values and percentage measures covering portfolio performance. (These should be developed for loans grouped by types or for entire portfolios.)
- Targeted ratios maintained for delinquency and charge-offs, NPAs, pass, criticized, and classified assets, and weighted average risk rating.
- Max forecast one year and CCAR[13] losses.
- Credit risk economic capital ratio.
- Granular data on borrowers by:
  - Type.
  - Industry (NAICS and SIC).
  - Risk rating.
  - Loss given default.
  - Probability of default.
  - Line of business.
  - Sales size.
  - Commitment.
  - Credit conversion factor – total exposure.
  - Credit conversion factor – unused commitment.
  - Collateral type.
  - Collateral coverage.
  - Amount of commitment (original and available).
  - Lien position on property.
  - Past-due days.
  - Nonaccrual indicator.
  - Default reason.
  - Actual exposure at default.
  - Date of default.
  - Date of default resolution.
  - Gross charge-off amount.
  - Net charge-off amount.
  - Recovery amount
- Concentration limits or maximum permitted exposures to a variety of categories:
  - Loan by certain type.
  - Geographic exposure.
  - Individual loan size.
  - Industry exposure.
  - Underwriting exceptions.
  - Leveraged lending.
- YTD average new original risk rate.
- Construction CRE (% risk-based capital).
- Non-owner-occupied CRE (% risk-based capital).
- % OREO > 1 year old.
- For new loans, expected loss rate through the cycle.
- Non-performing assets / total loan + OREO + LHFS ratio.
- Total classified loan / total loan ratio.
- Risk rating accuracy.
- Internal maximum credit limit as a percentage of total risk based capital to any one financial institution and its affiliates.
- Number of approved exceptions to aggregate guidance limits for institutions within a single sovereign based on risk rating of the sovereign.
- Exposure limits to institutions risk rated below investment grade as a percentage of the total portfolio.
- Number of defined segments with notional exposure or credit risk capital metrics exceeding concentration policy thresholds.

13 Comprehensive Capital Analysis and Review (CCAR) is an annual exercise by the Federal Reserve to assess whether the largest bank holding companies operating in the United States have sufficient capital to continue operations throughout times of economic and financial stress and that they have robust, forward-looking capital-planning processes that account for their unique risks. https://www.federalreserve.gov/bankinforeg/stress-tests-capital-planning.htm

- For all segments in aggregate, the total industry commitment exposure in excess of the concentration threshold.
- Original approvals with expectations exceeding house limits as a percentage of total commitments.
- Credit strategies are clearly articulated and approved through the credit committee, its subcommittees, and working groups.
- Credit policy exceptions are tracked and monitored; progress is reported regularly.
- Rational tolerances, limits, and targets are reviewed and monitored by the credit risk committee, supporting subcommittees, and working groups.
- Allowance maintained for loan and lease losses at a level that is adequate to absorb all estimated inherent losses through extensive governance.
- Criticized assets – max %.
- Non-performing assets – max %.
- Charge off rate – target range in basis points.
- ALLL – qualitative (e.g., maintain at an adequate level…).
- High level credit:
  - Classified/tier 1+ ACL.
  - Delinquency >60dpd.
  - Loan growth in major LOBs >10%.
- Gross charge-offs.
- Six-month PD downgrade trends.
- Classified asset ratio.
- Commitments by NAICS as % of RWA's and tier 1 capital.
- Satisfactory CAMELS ratings for asset quality achieved.
- NPAs (non-performing assets) / assets maintained within acceptable level (%).
- NPLs (non-performing loans) / loans maintained within acceptable level (%).
- ALLL maintained within acceptable level.
- Commercial real estate (CRE) loans/total RBC maintained within acceptable level (%).
- Residential 1–4 maintained within limits to RBC (%).
- C&I maintained within limits to RBC (%).
- Collateral quality.
- Legal entity exposure.

Culture:

- Workplace satisfaction surveys (number of business units/locations with ratings below goal).
- Average days to fill open position (recruitment).

Diversification and concentration:

- Risk-weighted assets by geography and type.
- Commitments by NAICS as % of RWA's and tier-1 capital.

Earnings and earnings volatility:

- Risk-adjusted return on capital (RAROC).
- Return on risk capital (RORC).
- Return on assets (ROA).
- Return on average assets (ROAA).
- Return on average tangible common equity.
- Core ROA.
- Efficiency ratio.
- Net interest margin (NIM).
- Profitability of new business units.
- Annual growth rate in earnings before taxes.
- Interest and taxes (EBIT) growth.

- Earnings concentration risk.
- New business opportunities to maintain or improve our risk/earnings diversification.
- Debt-to-equity ratio.
- Price-to-earnings ratio.
- Month-to-date ROA performance to target (set target ROA and allowable range above or below target).
- Volatility in annual stock return.

Liquidity:

- Regulatory liquidity ratio.
- Volatile dependency ratio.
- Liquidity coverage ratio.
- Crisis liquidity coverage ratio.
- Short-term purchased funds to assets.
- Large liability dependency ratio.
- Net stable funding ratio.
- Rollover risk concentration ratio.
- Total borrowed funds / total assets ratio.
- Brokered CD / total assets ratio.
- Targeted liquidity to maintain next 60 days.
- Months to required funding.
- Contingency funding ratio.
- Net maturities < = 30 days as a % of total assets.
- Holding company cash position decision tree status.
- Liquidity action options tree status.
- Long-term credit rating.
- Secured deposit / total deposits.
- Establish funding strategy that provides effective diversification in the sources and tenor of funding.
- Loans to core deposits ≤ X %.
- Loans to core plus insured deposits ≤ X %.
- Loans to core deposits plus insured deposits plus long-term debt ≤ X %.
- Excess liquidity ≥ X % of assets.
- Time to required funding.
- Liquid asset / total liabilities.
- Liquid asset / total deposits.
- Total wholesale funding / total assets.
- Total brokered and internet service deposits / total assets.
- Satisfactory CAMELS ratings for liquidity.
- Satisfactory net non-core funding dependence (%).
- Satisfactory net short-term liabilities / assets (%).
- Satisfactory FHLB funding availability.
- Acceptable levels of pledged securities.

Market:

- Net interest income at risk.
- Economic value of equity at risk.
- 12-month cumulative GAP.
- Aggregate trading value at risk.
- Duration of equity.
- Market risk economic capital ratio.
- Number of exceptions to maintaining a daily enterprise trading 10 day value at risk (VaR) ≤ $25 million (non-traded and traded).
- Change in one-year net interest income following a +/- 200 bps change in interest rates (non-traded).
- Change in economic value of equity following a +/- 200 bps change in interest rates (non-traded).

- Sensitivity of net interest income (NII) managed to mitigate exposure to adverse changes in interest rates through various scenarios that are regularly presented to ALCO for assessment.
- Major hedging or risk mitigation strategies are approved in advance by ALCO.
- Net interest income change within specific target range (e.g., no greater than plus or minus X %).
- Economic value of equity (EVE).
- EVE change – no greater than X%.
- EVE above acceptable levels with up/down 100, 200, 300 bps rate shocks.
- Net interest income at risk.
- Satisfactory CAMELS ratings for sensitivity to market risk.
- Duration gap above acceptable levels with up/down 100, 200, 300 bps rate shocks.
- Interest expense/ avg. assets within acceptable limits (%).
- Rate-sensitive assets/assets (%).
- Rate-sensitive liabilities/assets (%).

Market Indicators:

- House Price Index (HPI).
- Unemployment.
- 10–2-year Treasury yield curve spread.
- Cap rates for CRE.
- Lending standards via the Fed's senior loan officer lending survey[14].
- Agency rating upgrade/downgrade ratio for corporate.
- S&P leveraged loan price index[15].
- Spreads on securitized assets: auto, MTG, CMBS, card.

Market indicators are used to distill the tenor of the market and provide an early read on an impending change in the credit cycle.

Model Risk:

- Model identification and tiers.
- Inventory.
  - Assessment and reporting.
  - Development, testing, and documentation.
  - Independent review.
  - Validation.

Operational:

- Cyber security.
- Leading indicators for people, vendor management, processes, and systems.
- Total, expected, and unexpected fraud losses by type.
- Total float by payment type.
- Daylight overdraft limit with Federal Reserve.
- Operational risk economic capital ratio.
- % overtime to total budgeted payroll.
- Attacks to firewall.
- Failed phishing-awareness testing.
- Recovery of priority-one incidents.
- Recovery testing of critical applications.
- Critical business processes with inadequate business continuity plan.
- Third parties with inadequate recovery tests.

14 https://www.federalreserve.gov/boarddocs/snloansurvey/.

15 http://us.spindices.com/indices/fixed-income/sp-lsta-us-leveraged-loan-100-index.

- Data quality score.
- Critical models with unsatisfactory rating.
- Legal losses including settlements, attorney's fees, and regulatory fines.
- Quarterly operational losses as a percentage of quarterly net interest income plus non-interest income.
- Quarterly operational losses (enterprise wide).
- Active high models rated fail as a percentage of all active high models that have been validated.
- Number of unresolved significant deficiencies in internal controls over financial reporting identified in accordance with the Sarbanes-Oxley Act of 2002.
- Number of unresolved material weaknesses in internal controls over financial reporting identified in accordance with the Sarbanes-Oxley Act of 2002.
- An event where more than 100,000 customer or associate records, or significant bank intellectual property, has been compromised as a result of a system weakness or failure, including a cyber-attack or security breach by bank or its service providers.
- Number of technology severity events.
- Losses as a result of external malicious attacks.
- Employee fraud.
- Robbery.
- Deposit loss per account.
- Cybersecurity maturity ratio.
- Technology spend/revenue ratio.
- Maintain acceptable level of operational losses ($000s).
- Maintain high level of critical system availability (%).
- Maintain adequate insurance coverage (e.g. flood/hazard) (%).
- Maintain optimal level of employee headcount (%).
- Minimize confidential data breaches.
- Team members in countries of elevated risk of bribery or corruption.
- Model risk.
- Business continuity planning.

People and Compensation:

- Employee retention rate of top talent.
- Turnover rate.
- Vetting of business opportunities by the executive management committee.
- Culture that welcomes accountability, candor, and transparency through ongoing messaging and training.
- Avoiding unfavorable view by our stakeholders by identifying, responding to, and resolving customer complaints.
- Balanced scorecards for key positions.
- Succession planning in place for senior management/key personnel (%).

Reputation, Compliance, and Legal:

- Number of active litigation matters.
- Legal losses including settlements, attorney's fees, and regulatory fines.
- Open issues/MRAs.
- Trend in open or threatened legal matters.
- Community Reinvestment Act rating.
- Percent of associates who have completed mandatory compliance training.
- Number of outstanding Department of Justice referrals on compliance issues.
- Monitoring and testing activities align with required testing schedule based on residual risk rating.

- Number of items requiring management action trending behind schedule or past due
- Minimization of Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) related losses ($000s).
- Number of Office of Foreign Assets Control (OFAC) violations per quarter (including self-identified reported to OFAC).
- Number of business units with an adverse internal audit rating relative to BSA/AML/OFAC.
- Percentage of discovered BSA/AML deficiencies (included self-identified) involving currency transaction reports (CTR).
- Number of discovered BSA/AML deficiencies (including self-reported) involving unfiled suspicious activity reports (SAR).
- Problem incidence (percentage experiencing problem or annoyance in previous three months).
- Customer loyalty as compared to bank's peer group in Gallup's retail banking database.
- Branch customer experience score as compared to banks' peer group in Gallup's retail banking database.
- Retail banking satisfaction index score as compared to banks' peer group average in the JD Power's retail banking satisfaction survey.
- Media tone differential (percentage of negative news articles in excess of peer average).
- Customer complaints.
- Net promoter score.
- JD Power overall satisfaction score.
- New or open regulatory MRIA.
- High risk internal/external audit finding resolution.
- Number of internal audit reports less than satisfactory (%).
- Number of external audit reports less than satisfactory.
- Number of customer complaints.
- Number of new or proposed regulations or legislation.
- Achieve satisfactory CAMELS ratings for management.
- Community Reinvestment Act activities.
- Achievement of strategic goals.
- Avoidance of a financial restatement with the use of extensive controls around financial statements and reporting with oversight.

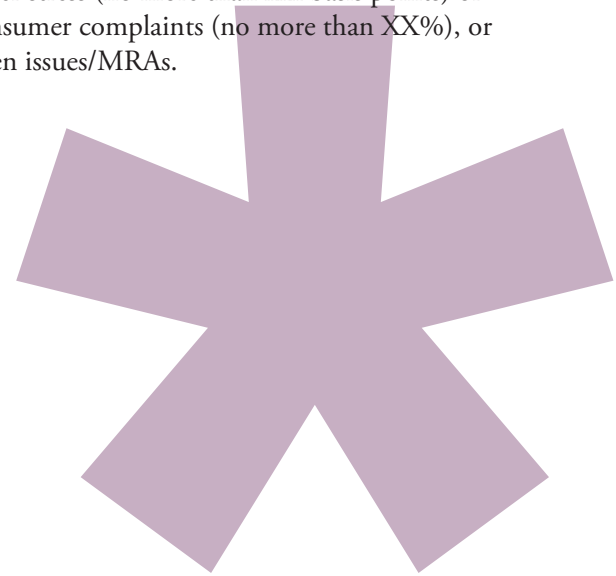
Strategic Alignment:

- Exposure to noncore relationships or businesses to be less than XX% of total exposure.
- Capital dedicated to noncore businesses not to exceed X% of total.
- Capital allocated to activities outside current expertise.
- Assets in noncore activities.
- New product.

Sustainability:

- Exposures in high-risk sectors such as chemicals, energy, forestry, and mining to RWAs and tier 1 capital.

In terms of actual limit setting, some institutions are moving toward a change-in-performance paradigm. For example, they use calculations such as change in tier-1 common under stress (no more than xxx basis points) or change in consumer complaints (no more than XX%), or change in open issues/MRAs.



XIV. COMMUNICATION: REPORTING THE RESULTS

Obviously, the results of any risk assessment process need to be interpreted, communicated, and acted on accordingly. But how this information is aggregated and presented can be meaningful in terms of how people receive and evaluate it. This section discusses strategies for maximizing the value and use of data acquired from risk assessments.

COMMUNICATING THE ASSESSMENT RESULTS

Regardless of which basis and method the institution chooses to develop its risk assessment, the final report should include the following elements:

- A risk profile for the institution at both a strategic/macro and operational level that also documents major risk types (strategic, credit, operational, etc.).
- A summary of the institution's top risks and their respective risk ratings, both in terms of inherent and residual risks.
- A list of any risks that are outside of acceptable tolerance values, or that could be strengthened without significant effort, and management's action plan for response.
- A list of any areas where controls have been determined to be insufficient accompanied by management's action plan for remediation.
- Management's overall conclusion about the risk levels, risk trends, emerging risk areas, and any additional recommendations for changes, particularly at a strategic level.

Again, many business staff are indifferent to enterprise risk assessments because they believe, "We already know the risks that can kill us." This is an unfortunate and shortsighted perspective on risk assessments. Just because a risk can't "end the bank" doesn't mean it shouldn't be evaluated, and if necessary, further mitigated. The sheer process of conducting these assessments improves awareness of risks, and significantly increases ownership and accountability towards risk, which can not only create frustrating and unnecessary losses, but can sometimes have devastating effects, particularly for smaller institutions. The trick is to design the correct assessment framework that is size appropriate for the individual institution. Remember, people can't manage risks they don't understand.

DASHBOARDS VS. NARRATIVES

In presenting information, should you use simplistic dashboards, detailed narrative, or some combination of both? The answer depends on the institution and how its management and board prefer to receive information. However, for information to be actionable, it must be digestible. A report with page after page of narrative is impossible to digest quickly and will not lead to quick decision making. Alternatively, simplistic dashboards without associated narratives are easily misinterpreted and may lead to decisions that do not consider all relevant factors. The most effective approach is to combine a top level dashboard with a brief narrative that summarizes the results of the assessment and suggested action items. The information should be supported by a more detailed narrative for those that choose to dig deeper.

Remember, the purpose of an assessment is to help you determine if the bank is operating within the guardrails of 1) its strategic plan and 2) its risk appetite. A macro-level assessment provides information about how closely the institution is adhering to its strategic plan and an operational assessment provides information about whether the institution is operating within the bounds of its risk appetite. If the risk assessment report does not provide this information, further assessments are necessary. Emphasis should be placed on trends or patterns because single results can be isolated issues.

RISK COMMITTEES

When it comes to overseeing the Enterprise Risk Management program, and enterprise risk assessments in particular, Risk Committees play a key role. While the first draft of any risk assessment should be reviewed and interpreted by the individual managers overseeing each area of the institution, at some point the executive team should review the results to determine whether the risk profile is as expected and to understand what areas may require additional remediation. The Management Risk Committee (typically executive management) should be reviewing the information in some detail to confirm that they agree with the results and subsequent action plan. The Board Risk Committee should review the executive summary and key assumptions in order to provide challenge to management on the assessment findings and overall risk profiles. Both committees should continually ask, “Are we within the guardrails?” And both risk committees should receive regular reports on the state of remediation efforts and any updated risk profiles based on those remediation efforts.

Communication is the most critical step. No matter how fully developed or supported the framework, metrics, inventory, or translation is, ERM cannot make an impact unless it is effectively communicated. Factors that can impede effective communication include personality types (enablers, blockers, silent assassins, etc.), unfettered access to the board of directors or its risk committee, and the enterprise culture.

EXECUTING THE STRATEGY

Following are suggestions for how to execute an effective communication strategy:

- Take a big-picture assessment of your corporate culture and whether it varies by risk or risk group. For example, some companies attempt to reduce risk with a level return, others accept increased risk for an increased return, and some seek to level risk for a level return.
- Avoid broad terms and be specific on accountability for the risk source, change-agent individuals and groups, and dates. Lead by example.
- Keep the "on the record" materials to a minimum at the start. Meetings typically need minutes, but there should be a reasonable balance between documenting the topics discussed and transcribing what was actually said. Open dialogue is the key.
- Evaluate the frequency and methods of communication regularly. Closely balance the ERM learning curve, need for risk mitigation, and key constituent availability with the potential for losing relevance.
- Liven up the communication strategy with job aides, audio/visual materials, playing cards, games, or other nontraditional communication methods.
- Consider dividing the audience into groups when discussing risk appetite and tailor the communication to each. Distinguish between the appropriate communication for the board of directors and for the business line. You want business units to understand the risk appetite and be able to apply it, translating the appetite all the way down to behaviors in role-specific functions. This approach should ensure that the total message is received and applied.
- Provide the ERM department with tools and reports built around the risk appetite that both communicate the appetite and measure performance. Not all tools are appropriate for every audience. Some can be too high level and others too granular. Thus, the ERM department should create specific reports for each group. The reporting should be done in conjunction with input from the senior management team and board of directors.
- Give visibility to the risks that matter. Where do we need resources? Where do we have under-controlled risk? Where are we over-controlled?
- Develop a common language for discussing risk. This ensures a common way to identify risks and discuss them within the institution.

Ways to communicate risk include risk appetite statements, lists of top organizational risks, risk category heat maps, incident tracking (highlighting mistakes), and key performance indicators (providing a proactive look at potential issues).

Heat maps draw attention to what needs to be focused on. Activities that are coded red, yellow, or orange will generate dialogue around why those colors are in effect and which actions are being taken to align risk levels with the risk appetite statement. Trend reports also help focus attention on, for example, whether activities are trending away from green and if they should be monitored more closely. Key performance indicators also help provide a proactive view.

XV. SUMMARY

Enterprise risk management creates real value for the enterprise, making an institution more competitive and more profitable, while contributing greatly to its safety and soundness. Risk measurement, evaluation, and communication are critical pieces of an enterprise risk management framework. You must understand risk in order to manage it. And to understand it you must be able to quantify it and mitigate it with controls.

The risk measurement process helps you to create risk metrics, which ultimately inform the risk appetite. Begin by establishing basic risks to be measured with the understanding that the process is fluid, and you can make adjustments later. Although you can use alternative approaches to size risk, all approaches must consider the risk's severity, likelihood, and frequency.

Risk identification is key. Make sure your institution has a comprehensive and repeatable process to identify material and nonmaterial risks throughout business lines, products, and services. The process is critical to downstream efforts on sizing, setting limits, monitoring, controlling, and reporting risks. Once risks are identified, management has to allocate its scarce resources to measuring risk and optimizing the measurement approaches to cover the largest and most complex risks.

When building an enterprise or operational risk assessment, you must determine the focal point of the assessment, also known as the assessment foundation or basis. You then need to determine the approach or level of detail that you need. The two most common structures for a risk assessment are either based on risk types (strategic, credit, liquidity, market, interest rate, or operational risk) or on enterprise details such as strategy and process.

FOUR PHASES OF RISK MEASUREMENT

Effective risk measurement typically undergoes four evolutionary phases. The measurement phase takes into account data collection, storage, and fabric. During the theory building phase, management observes and categorizes events with the intent to explain the cause of the observed events. In the risk sizing phase, management decides the method or combination of methods it will use to size the risks. Those include intuitive/judgmental method, the likelihood/impact method, and the quantitative method. In the governance phase, risk appetite serves as the basis for all risk governance decisions and actions. Because the process of risk sizing directly supports factual, objective, consistent, and repeatable risk management, risk sizing also supports the definition and ongoing calibration of risk appetite.

MANAGING RISK ACROSS THE ENTERPRISE

The purpose of a defined risk framework is to articulate the firm's risk tolerances and to monitor and control those risk exposures against established limits. The framework should define and manage individual and aggregate risks so that the firm does not exceed its established risk appetite. A risk appetite framework should include at least the following key components: statement of the stakeholders' risk objectives, measures and/or metrics to establish and measure risk tolerances, and limits structures.

Everyone in the organization needs to understand the bank's risk appetite and its commitment to managing risk across the enterprise. Stephen Phillips, EVP and Chief Banking Officer, First United Bank, Durant, Oklahoma, stressed the importance of everyone in the organization understanding the bank's risk appetite and its commitment to managing risk across the enterprise in an interview with The RMA Journal. "It's all about visibility," he said. "In my experience, people don't focus on certain things because they don't feel there is any real value to it. The more that we as an industry can show that there is real value in enterprise risk management, that there is a competitive advantage, and that it prevents the risk of dollar loss and reputation loss, the easier it will be for people to get on board with it."[16]

16 Stephen Phillips, "The Journey to ERM," The RMA Journal, July-August 2015.

APPENDIX: BRIEFING TEMPLATE FOR EMERGING RISKS

Briefing: X.X.X
Topic: *Add topic name*
Date: *Add date*

Risk Rating: *Insert risk rating*
Type of Risk: *Circle level and category*
Level: Primary Secondary Tertiary
Category: Market Idiosyncratic

Participants:

Add the list of participants.

Executive Summary:

Briefly describe the issue, the impact and/or likelihood, and response to the topic.

Impact Analysis:

Risk pillars.

Pillars	Affects (Y/N)	Primary Risk	Secondary Risk	Tertiary Risk	Drivers
Credit	*Is this pillar affected?*	*Is this a primary risk?*	*Is this a secondary risk?*	*Is this a tertiary risk?*	*What are the drivers of this risk pillar?*
Compliance					
Legal					
Liquidity					
Market					
Operational					
Reputational					
Strategic					

Income statement

Only required for primary risk briefings (not applicable for secondary and tertiary risk briefings)

Income Statements	Likelihood (%)[17]	Impact ($)[18]
Spread Interest Income	*What is the Likelihood?*	*What is the Impact?*
Direct Fee Income		
Security Gains (Losses)		
Personnel Costs		
Other Expenses		
Provision Expense		

17 Likelihood Scale: < 10%; 10% - 20%; 20% - 50%; 50% - 75%; >75%.
18 Impact Scale: <$0.5MM; $0.5MM – $1.0MM; $1.0MM - $15.0MM; $15MM - $40.0MM; >$40MM.

Balance Sheet

Only required for primary risk briefings (not applicable for secondary and tertiary risk briefings)

Balance Sheet	Likelihood (%)	Impact ($)
Commercial Loans	*What is the likelihood?*	*What is the Impact?*
Consumer Loans		
Securities – AFS		
Securities – HTM		
Deposits – Consumer		
Deposits – Commercial		
Other Borrowing		

Control/Response Strategy

What are the control and/or monitoring responses for this risk?

Other Salient Data

What other salient data should we consider in our analysis?

Conclusion

What is the conclusion on how to monitor and/or mitigate this risk? What is the likelihood of the risk materializing and how would it
impact the firm?

Next Steps

- *Future triggers:* What futures triggers should be monitored?
- *Consequences of being off-target:* What are the consequences of being off-target in our assessment?
- *Next update:* How and when should we determine the next update to this briefing?

