rma
THE RISK MANAGEMENT ASSOCIATION

GOVERNANCE AND POLICIES WORKBOOK

JOIN. ENGAGE. LEAD.

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

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 principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues. Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

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

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.

While RMA believes the material contained in this publication is accurate, the conclusions and opinions expressed are those of the authors. Moreover, no opinion expressed on a legal matter should be relied on without the advice of counsel familiar with both the facts in a particular case and the applicable law.

This material is part of RMA's educational resources for commercial bankers at every stage of their careers. For more information, contact the Customer Care Department, RMA, 1801 Market Street, Suite 300, Philadelphia, PA 19103. Or contact us by: Phone 800-677-7621 / Fax 215-446-4101 / E-mail courses@rmahq.org or our website: www.rmahq.org.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

RMA wishes to acknowledge the work, thoughts, and contributions of the Governance Workbook working group. To the members of this group, RMA extends its appreciation:

GOVERNANCE WORKBOOK WORKING GROUP

Nancy J. Foster*

EVP/Chief Risk Officer

Park Sterling Bank

Jennifer O'Reilly*

SVP/Risk Reporting & Analysis

Union Bank

Edward P. Schreiber*

EVP/Chief Risk Officer

Zions Bancorporation

Yousef Valine**

EVP/Chief Risk Officer

First Horizon National Corporation

* Enterprise Risk Management Council Member
** Enterprise Risk Management Council Chair

RMA also thanks the members of the Enterprise Risk Management Council for their help in developing, guiding, and reviewing the Governance and Policies Workbook:

ENTERPRISE RISK MANAGEMENT COUNCIL

Amy D. Cook	Capital One National Association
Nancy S. Crooks	Union Bank National Association
Christine Eagan	Columbia State Bank
Kathleen A. Flannery	PNC Bank NA
Debra S. Fournier	Bank of the West
Heidi M. Gillespie	EverBank
Michael L. Gunnels	American National Bank of Texas
Helga Houston	Huntington National Bank
Joseph A. Iraci	TD Ameritrade
Nigel Murtagh	Charles Schwab & Co. Inc.
Jacqui M. Peace	USAA Federal Savings Bank
Thomas M. Petro	Fox Chase Bank
Bruce A. Schouten	Toronto Dominion Bank

RMA would also like to thank the Federal Home Loan Bank of Atlanta for their contributions to the Workbook.

SPECIAL THANKS

RMA extends a special thanks to Eric Holmquist, Managing Director, Enterprise Risk Management, Accume Partners, for contributing content, technical advice, and practical insight.

Eric is an active supporter of RMA's enterprise risk management practice. His work with RMA over many years has covered a wide range of subjects including risk management, operational risk, and governance.

Eric serves on the Editorial Advisory Board of *The RMA Journal*. He has authored *Journal* articles, led conference presentations, and delivered audio conferences on behalf of RMA.

PREFACE

WHAT IS ERM?

Although the concept of enterprise risk management (ERM) has existed for a number of years, it wasn't until the 2008 financial crisis that ERM gained prominence as an integral part of an institution's overall business strategy.

Despite the increased focus on ERM, many in the industry struggle to define it precisely. As a result, RMA's ERM Council embarked on an effort to create highly practical guides for implementing a robust ERM framework that will help institutions of any size manage their risks holistically.

The council defines ERM as "the management capability to manage all business risks in pursuit of acceptable returns." With that definition as a guide, the council adopted a strategy that will help management and boards answer relevant business questions pertaining to an institution's risk appetite, business strategy and risk coverage, governance and policies, risk data and infrastructure, measurement and evaluation, control environment, risk response, and stress testing.

At the center of the ERM framework is culture. If an institution lacks the right culture and strong leadership at the top, none of the other elements may matter. Simply put, firms that comprehend and adopt ERM as a way of thinking likely are on a path to outperforming those that do not.

Ultimately, ERM can provide an institution's board and management with answers to three basic business questions:

1. *Should we do it?* Is our ERM program aligned with business strategy, risk appetite, culture, values, and ethics?

2. *Can we do it?* Do we have the people, processes, structure, and technology capabilities?

3. *Did we do it?* Do we have in place an assessment of expected results, continuous learning, and a robust system of checks and balances?

INTRODUCTION

RMA'S ENTERPRISE RISK MANAGEMENT FRAMEWORK

The ERM framework was designed to help managements and boards of directors answer these relevant business questions (the terms in parentheses are the components that will help in addressing them):

1. What are all the risks to our business strategy and operations? ***(coverage)***

2. How much risk are we willing to take? ***(risk appetite)***

3. How do we govern risk taking? ***(culture, governance, and policies)***

4. How do we capture the information we need to manage these risks? ***(risk data and infrastructure)***

5. How do we control the risks? ***(control environment)***

6. How do we know the size of the various risks? ***(measurement and evaluation)***

7. What are we doing about these risks? ***(response)***

8. What possible scenarios could hurt us? ***(scenario analysis)***

9. How are our key assumptions affected under changing conditions? ***(stress testing)***

10. How are various risks interrelated? ***(scenario analysis & stress testing)***

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

7/13

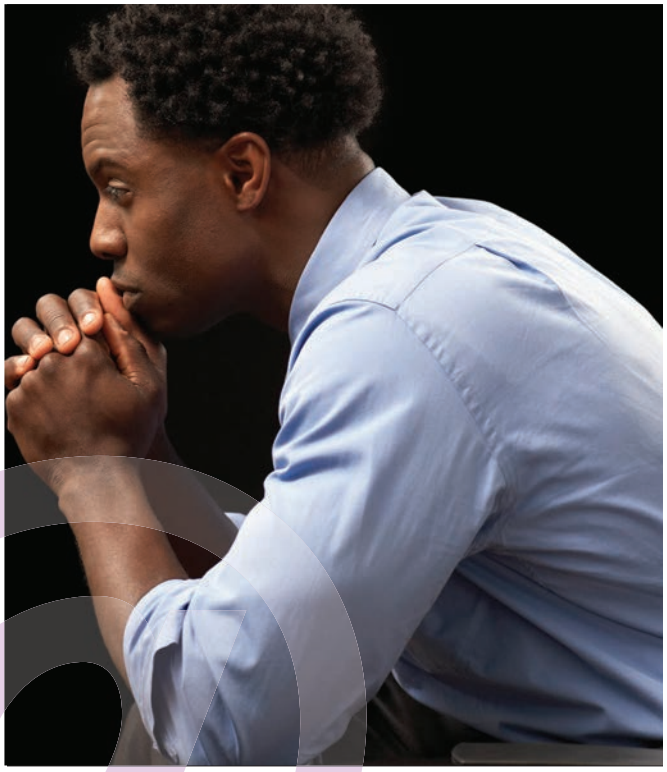
JOIN. ENGAGE. LEAD.

The framework applies regardless of the 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 represent a dynamic flow in both directions. Additionally, culture is depicted as the center or heart of the program, since without the right culture the other components are of dubious value.

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

As part of its approach to developing this ERM framework and associated ERM competencies, RMA's ERM Council is developing a series of practical workbooks for risk management professionals. The workbooks are as follows:

1. Risk Appetite (published November 2010)
2. Governance and Policies (addressed in this workbook)
3. Risk Data and Infrastructure (to be developed)
4. Measurement and Evaluation (to be developed)
5. Reponses (addressed in this workbook)
6. Stress Testing (published February 2012)



CHAPTER ONE - GOVERNANCE

This chapter provides an overview of core capabilities required for a strong risk governance culture, structure, policies and procedures, and internal control environment. Chapters 2 and 3 provide further details on culture, and the internal control environment/response capabilities.

Strong governance can help a firm ensure that:

- The risk appetite implicit in the company's business model, strategy, and execution is appropriate.
- The expected risks are commensurate with the expected rewards.
- Management has implemented a system to manage, monitor, and mitigate risk, and that system is appropriate given the company's business model and strategy.
- The risk management system informs the board of the major risks facing the company and how they are being managed.
- An appropriate culture of risk awareness exists throughout the organization.
- There is recognition that management of risk is essential to the successful execution of the company's strategy.
- A well-developed capital plan is in place to support the established risk appetite and strategic plan.
- A stress-testing program is in place to help determine sufficient capital availability based on the bank's strategic plan and risk appetite.

CULTURE

A strong risk management culture accomplishes two organizational objectives, summarized as follows:

1. *It helps the company make well-informed decisions.* A company with a strong risk management culture promotes, encourages, and rewards behaviors that avoid a "herd mentality," "confirmation bias," or "groupthink." It helps the company make better decisions because candor, transparency, and debate are demanded, encouraged, and incented. Everyone in the company sees risk management as part of their responsibilities and accountabilities. A system of checks and balances is understood and welcomed. Lack of credible challenge and debate in a financial services company (at the board level and/or management level) significantly increases the risk of disastrous outcomes. Knowing how to build a risk management culture that overcomes cognitive biases is challenging, but a requirement for a sound risk management and governance program.

2. *It helps the company identify rogue individuals and/or groups*. It is said that 99.9% of people show up to work every day intending to do the right thing. Sometimes these people make bad decisions not because they want to, but because of flawed thinking. However, there are times when individuals or groups (the other 0.1%) are more interested in their own personal gains than in doing what is right. In such cases, a strong governance and risk management culture tends to ensure that individuals conform to the culture or are eventually asked to leave. The reward is an environment in which people become the company's collective strength as they work toward a common goal rather than individual interests.

STRUCTURE

In governance, structure is all about information flow, escalation, decision making, and accountability. A typical governance structure has the following components:

1. *Board of directors and its committees:* There are many ways a board can organize itself to ensure that it has met its fiduciary responsibilities. For example, a financial institution may decide to have separate risk and audit committees (Dodd-Frank requires this for institutions with more than $10 billion in assets). Alternatively, in smaller institutions there may be only an audit committee that oversees risk taking. Regardless of how a board decides to organize itself, the important objective is to have a robust governance structure for risk taking. Below is one example of how a board of directors has decided to provide coverage:

RISK COVERAGE AND OVERSIGHT

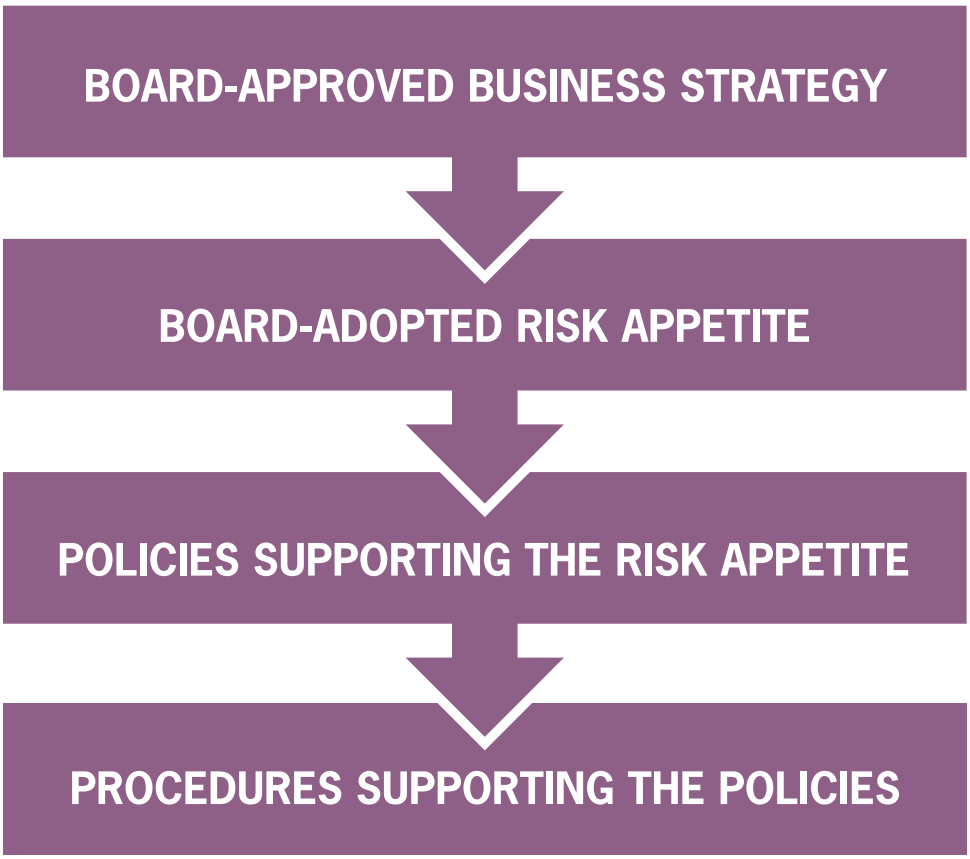
BOARD OF DIRECTORS

- Business strategy / risk appetite
- Reputation
- Liquidity
- Credit
- Fiduciary
- Operational
- Market
- Interest rate sensitivity
- Compensation/pension/savings plan/succession
- Financial

EXECUTIVE AND RISK COMMITTEE	AUDIT COMMITTEE	COMPENSATION COMMITTEE	NOMINATING CORP. GOVERNANCE COMMITTEE	TRUST COMMITTEE
- Risk appetite - Credit - Operational - New products - Compliance/legal - Interest rate - Liquidity - Market	- Financial - Disclosure - Internal controls and audit - Annual compliance report	- Compensation - Pension - Savings Plan - Compliance with labor laws - Succession planning	- Corporate governance - Board and management evaluation - Director nomination	- Exercise of fiduciary authority - Oversee fiduciary operations - Fiduciary policies

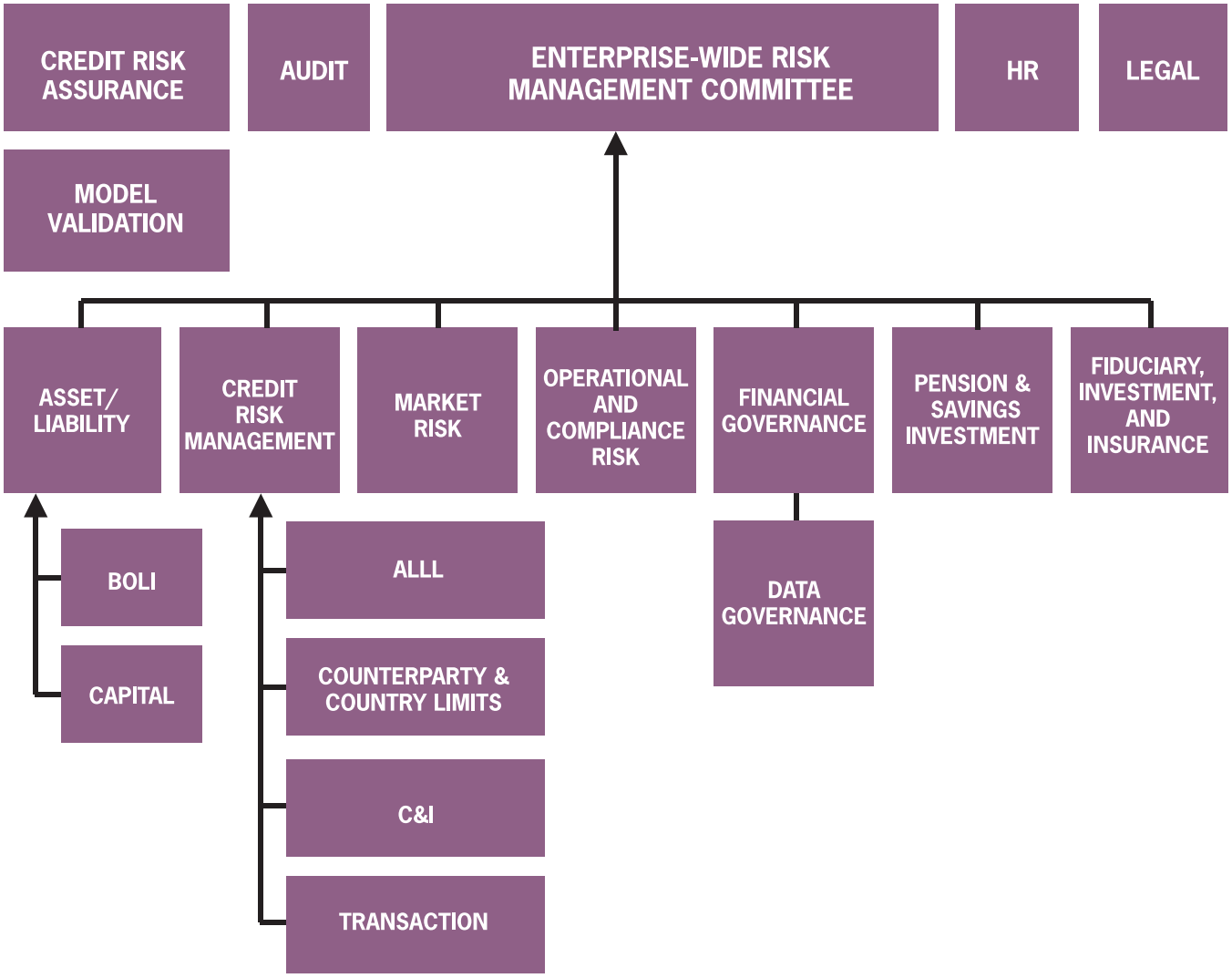
Examples of charters for board-level committees are included in Appendix B.

2. *Management committees:* Management is required to operate with board-approved business strategies, risk appetite, and policies. The process may be depicted as follows:



Similar to a board committee structure, management has flexibility in organizing its management committees to oversee risk taking. The flow chart below shows how one institution has organized itself:

RISK GOVERNANCE STRUCTURE



In this example, data governance is included under financial governance. However, managing data is a process that is overseen by all of the committees listed above.

Other examples of board-level committee structures are included in Appendix A.

GOVERNANCE: THE DIFFERENT ROLES

The Board of Directors:

- Do the board members have a good grasp on risk appetite and risk alignment?
- Are risk profiles at the macro and micro level providing the board with high-level information and key risks of concern?
- Is the board receiving risk reports that are informative and actionable?
- Is training for board members needed? (If so, do it.)

The Board Risk Committee:

- Are the members of this committee the ones who understand risk?
- Is the committee charter the appropriate one?
- Is the agenda forward looking or just a summary of past results?
- Do the committee members know what they should be looking for?
- Do they know what questions to ask?

The role of the Chief Risk Officer is to help with "know" rather than "no"

The Chief Risk Officer:

- This position cannot be Internal Audit II; it should be independent, reporting to the board risk committee and living in the gray space between internal audit and the lines of business.
- The CRO approves policies and processes, not proposals.
- This position owns the risk management program, not the risk.
- Subject-matter expertise is critical, but can be supplemented.
- The CRO should sign off on whether the process for new programs is being followed but not the programs themselves.

The Management Risk Committee:

- Are the members the right ones to be serving on this committee?
- Is the charter appropriate for the mission?
- Is the agenda forward looking?
- Does transparency rule?
- What experience does each committee member have?

POLICIES AND PROCEDURES

Policies communicate and reflect the company's risk appetite to all stakeholders. They describe what the company is willing to do and not willing to do. The statement of risk appetite is operationalized through policies ("What should we do?") and procedures ("How should we do it?"). Policies should be brief—no more than two or three pages—and express the following:

1. *Overview of the policy:* What is it intended to accomplish?

2. *Authority:* Who is accountable for implementing the policy?

3. *Implementation:* How will the policy be implemented?

4. *Exceptions:* How should exceptions be handled?

Procedures are highly specific. They describe in detail how the policy will be executed. And they should be written at a level that allows them to be audited or tested.

How an institution approves its policies and procedures is a matter of preference. Generally, the policies, since they are expressions of the board-approved statement of risk appetite, are approved by the board of directors or its designated committee. The procedures are approved by the appropriate management group that is responsible and accountable for their execution.

The most important ingredient in execution is communication and incorporation of policies and procedures into day-to-day processes and technology. The best policies and procedures are useless if they are communicated ineffectively and do not fit into the design and execution of the business processes. Additional information on policies and procedures is available in Chapter 3.

CONTROL ENVIRONMENT

Those controls that are instituted by management to help manage, mitigate, and/or hedge risks are encompassed in the definition of the control environment. Controls extend to committees, policies, procedures, processes, limits, monitoring, measurement, reporting, stress testing, concentration analysis, and so on.

Controls help manage what can be managed—in other words, the places where management can exert 100% control. Management cannot control what the Federal Reserve does with monetary policy, nor can it stop hurricanes. But management can build controls and response plans to help mitigate these uncontrollable risks. Chapter 3 discusses this very important topic.

A Blue Ribbon Commission of the National Association of Corporate Directors developed the following list of questions that can help boards and managements focus on what matters and articulate what a good ERM capability can achieve.

1. What is our corporate strategy aiming to accomplish—and how?

2. Which alternative strategies have been considered or explored?

3. Do the directors receive risk information in prioritized and actionable summaries?

4. Are the risks associated with business units presented to the board in a comprehensive, holistic manner?

5. How do losses that have occurred compare to the risks that have been identified? Are the losses consistent in magnitude and frequency with expectations given the risk profile presented to the board?

6. Can management and the board tie profits, as well as losses, to the presented risk profile?

7. How actively are resources (such as capital, balance sheet, and talent) being redeployed? Does the organization consistently, and on a timely basis, feed its winners and starve its losers?

8. What could go wrong or derail our strategy? For example, could multiple problems arise simultaneously or sequentially, resulting in a "perfect storm"?

9. Has management been forthcoming about any differences among senior leadership regarding strategic recommendations and decisions?

10. What are the assumptions underlying our strategy? And which of those assumptions could change or be wrong?

11. Which processes did management use to develop strategy and identify risk?

12. Have we achieved a common understanding of which triggers bring an issue to the board's attention?

13. Which capabilities are required to address risks? Where do we have gaps in capabilities?

14. Is there a common understanding among management, the board, and board committees about their respective roles, responsibilities, and accountabilities in the areas of strategy and risk oversight?

15. Does the board have a clear understanding of where strategy and risk oversight are delegated and which processes are used within management and among business units?

16. Do the board and committees discuss risk appetite with management?

17. How can discussion about risk appetite become part of the board's regular routine?

18. Are the board and the appropriate committees meeting regularly with the Chief Risk Officer (CRO)?

19. Has the board ensured that the CRO and general counsel have adequate resources and appropriate reporting lines to bring any changes in material risks to the board's attention?

20. Does the board have the appropriate committee structure for its significant oversight obligation in the risk area?

21. Does the board have sufficient personnel (including advisors) and financial resources in place to fulfill its risk management responsibilities?

22. Has the board adopted a leadership structure that ensures independent directors have a clearly defined leader?

23. Do the board and appropriate committees have access to the information they need to provide oversight in troubled financial times?

24. Have the board and the appropriate committees reviewed the incentive structure with strategy and risks in mind?

25. Have the board and the appropriate committees reviewed board composition and director skills to be assured of up-to-date competencies for overseeing the company's strategy, business lines, and material risks?

SUMMARY

When combined with appropriate policies and a strong culture, governance helps an institution manage its risk-taking activities. Although several examples are provided here, there is no "right" governance structure. Ultimately, each institution must determine which structure is best suited for its organization. Whether the CRO has a solid reporting line to the CEO and a dotted line to the board's risk committee or vice versa, the most important aspects are that the structure and the organization's culture support the flow of information, the escalation of concerns, appropriate decision making, and, finally, accountability.

CHAPTER TWO - CULTURE

Why do good people make bad decisions? Why do so many financial institutions fail? Why does the financial services industry repeat the same mistakes? How can we avoid the mistakes of the past? Do things like policies and procedures matter if people aren't held accountable for them?

These are basic questions but very complex issues. Many factors contribute to poor decisions that ultimately lead very knowledgeable, ethical, and hardworking people down the wrong path. We believe the surest way to a financial institution acheiving its financial and strategic objectives begins with a sound governance framework enhanced by the appropriate business execution and risk management culture.

This chapter outlines the critical components of a risk management culture. At a minimum, a strong risk management culture needs to include governance, policies, independent reviews, a robust system of checks and balances, and a culture that helps avoid strategic mistakes due to the underlining causes, which can range from "me first" to "herd mentality."

CULTURE: WHAT IS IT AND WHY IS IT IMPORTANT?

Each institution is a living organism made up of wholly unique individuals, each with their own agendas, belief systems, priorities, and perceptions. An institution is constantly changing, managing to a multitude of priorities and constituencies, and is, at any given point in time, only a few annual reports away from success or failure. It is the people of these organizations who represent, overwhelmingly, the single biggest factor in either achieving that success or experiencing failure. And this is where the challenge—and opportunity—lies.

> Culture can be described as what people do when they are not being watched.

People are the single biggest wildcard when it comes to whether risk is managed or ignored. It's simply not possible to have enough rules and procedures to cover every conceivable incident that could come up on a daily basis. **No amount of process can become a substitute for good judgment.**

What's needed, in addition to policies and procedures, is an environment in which people have a clear understanding of what they are trying to accomplish and what the guiding principles are that dictate how it gets done. It is in the company's best interest to create an environment in which people are allowed to ask hard questions like, "Is this a problem?" or "Why are we doing it this way?" Finally, a good risk management culture reinforces the fact that managing risk is everyone's responsibility, not just the supervisor's or internal audit's or risk management's, but everyone's.

HOW DO YOU BUILD A ROBUST ERM CULTURE?

The governance framework and process are critical to the establishment of culture, but the process starts with senior and executive management, the people who set the proverbial "tone at the top". And it's not just what these people say but, more importantly, what they do. People see, people do. Therefore, senior management needs to come to a consensus on what the company values are, and they need to live those values every day without exception.

> "Sound risk cultures don't just happen. They result from training, reinforcement, and shared objectives."
>
> Carolyn G. DuChene, Deputy Comptroller for Operational Risk, ABA Risk Management Forum, April 25, 2013

Similarly, the board and senior management need to develop clearly articulated statements about risk appetite and tolerance that spell out, unequivocally, the company's philosophy on risk acceptance. These statements should be developed such that they not only inform strategy, but can be operationalized and ensure that risk acceptance is treated consistently from the top of the organization to the bottom.

Creating a strong culture means asking hard questions about how information moves, who the facilitators are, and who creates impediments. This requires a clear understanding of how processes work, as well as which communication conduits need to be in place to properly facilitate those processes. Any hint of a breakdown in communication or process needs to be dealt with quickly and decisively. A culture of accountability is essential to ensuring that corrective action is taken to deal with those situations and prevent repeatable mistakes in the future.

AVOID CONFIRMATION BIAS

Instead of asking "will our controls work" ask "under what conditions will we not be able to manage this risk".

When it comes to risk management programs creating an appropriate risk culture, it is important to understand that a good risk management program will not automatically create a good risk culture and that a good risk culture does not automatically create a good risk program. Both have to be developed carefully and deliberately over time.

Ultimately, risk culture rises and falls on the concept of empowerment—giving people the tools and the training to be able to identify risk, assess it, evaluate it against the desired level of risk tolerance, and make decisions about suitable risk treatment. A cultural norm of "be quiet and just do your job" will never build a good risk management culture. In this sense, there is a distinct difference between a culture of empowerment and a culture of compliance. If minimum requirements are all that are communicated to employees, than that is the level to which they will perform. Alternatively, if people are trained in the concepts of risk management, not only may they meet compliance requirements, but they may also find creative methods for reducing risk and could ultimately take more ownership in the processes they support.

THE ESSENTIAL ELEMENT OF GOOD RISK MANAGEMENT CULTURE

While the idea of risk management culture can be difficult to define, it is easy to observe. A number of elements can be attributed to a strong risk culture, and by recognizing them we can consider ways to strengthen and improve that culture. As you view this list, think about your own company and whether the elements described have been deliberately considered and whether they reflect the culture within your own organization.

- Awareness is a common understanding of the company's mission, corporate values, and operating rules. It leads to a continual exploration of risks and opportunities, without the fear of ridicule or censorship. Awareness means:

  - A common understanding of the company's values and goals. What does success look like? What is important to the company and why is it important?

  - A common acceptance of the company's ethics. What is considered correct behavior and what is unacceptable? How are ethics violations to be reported? And what happens to those who violate those ethics?

  - A clear articulation of risk appetite and tolerance through policies and procedures. How much risk is the company willing to assume in the pursuit of its goals? And what are the means to measure that risk tolerance?

  - A common knowledge of the risks that exist throughout the organization. What are the treatments in place to (theoretically) address those risks in order to align them with risk appetite, policies and procedures?

  - A clear understanding of roles and responsibilities. Everyone has a specific job to do, and they need to understand not only what they are supposed to do, but why they are doing it.

- Communication systems must be in place to effectively move information throughout the organization. This means:

  – Mechanisms to capture institutional knowledge—so that, ideally, when something is learned, it is learned once and shared with others.

  – Structures for reporting, without criticism or condemnation, issues such as ethics violations, suspicious activities, control violations, evidence of elevated risk, and similar dangers. People are empowered to speak up without fear that someone will "shoot the messenger."

  – Information flows from the top down and from the bottom up, with limited filters and restrictions. A person's knowledge is more important than his or her perceived image or standing in the company.

- Transparency describes an environment in which people can be open about risks, abilities, limitations, and failures. It means:

  – Seeing failures as learning opportunities, where people are encouraged to learn from their mistakes and the mistakes of others and to ask good questions about how things can be improved.

  – Being able to openly discuss risks in order to find solutions. If someone knows that a given process is flawed or sub-optimal, they aren't afraid to say something for fear of retribution.

  – Discussions that focus on opportunity for improvement, not on whom to blame. In fact, the word "blame" cannot exist in the lexicon of the risk manager (that should be left to HR to manage). Instead, the focus should be on continuous improvement.

> "The best cultures and credit systems are simple and easily grasped. The measure of their quality is eventually seen on the bottom line."
>
> Mueller, P. Henry and Sihler, William W.
>
> *Realism in Lending, Anchor Your Bank to a Sound Credit Culture.*
>
> Philadelphia, The Risk Management Association, 2011.

- Accountability is ownership of goals, processes, risks, controls, etc. It is held by everyone. The idea is to be accountable for outcomes instead of looking for others to blame. Accountability starts at the top. If people see the executives looking for "the fall guy" when things go wrong, they will do the exact same thing. If they see people taking responsibility for their actions and the actions of their staff, then that is what they will do. Accountability means:

  – When things do go wrong, the person who was responsible is given the first shot at suggesting what could be done differently next time.

  – When people knowingly violate the values, ethics, and rules in the company, the issues are dealt with promptly and decisively. If employees observe that people get away with things, then they will try to do it as well.

- Cooperation is a cultural willingness to help others rather than wait for others to help you. In other words, it is a culture of service. It means:

  – People share a desire to work together to achieve a common goal, and the success of the company is more important than the success of the individual.

  – Someone who is clearly capable but still short on experience is seen as an opportunity to mentor, not as someone to criticize and marginalize.

  – Departments respect what the others do, never viewing their own contribution as more significant than those of the others. Instead, all departments are part of the whole.

- Agility or adaptability is the ability to change and adapt as circumstances change and the rules need to be adjusted. It means:

  – You don't keep doing things the way you've always done them even though it is obvious to everyone that the old ways aren't working.

  – The company asks hard questions about whether the strategy is working—and if is not, then what should be done about it. Then the company executes on it.

  – While there are clear lines of authority and approvals, people are empowered to make decisions and then act on them. Making changes takes days, not weeks or months.

The effects of risk culture are obvious, whether for good or for bad. An environment with a lack of motivation, where operational errors are constant, or where staff just put in their eight hours and feel like they never know what's going on will always lead to sub-optimal performance. But one in which people are engaged and enthusiastic, where they are aware of change long before it happens, where continuous improvement is not only encouraged but rewarded, and where people share a common sense of purpose leads to companies that outperform their peers, retain better, more qualified staff, and see greater profits. We may not be able to easily define risk management culture, but we definitely know it when we see it.

BARRIERS TO A GOOD RISK CULTURE

Building a healthy, dynamic risk management culture is a very positive thing, but it comes with a great number of obstacles and challenges. This section lays out some of these obstacles and signs that the risk management culture needs to improve.

- *Poor communication:* Too many companies operate on a "need to know" basis, and some accept the idea that not many people need to know. While there is no question that some information should be limited to certain individuals, most organizations err too far on the side of restricting information. The problem is, when people lack information, they make it up. And what people tend to make up to fill the void is almost always wrong, sometimes spectacularly so, resulting in a great deal of time wasted pondering it and even acting on it. A lack of information or misinformation can only degrade a culture.

- *Poor communicators:* It is a rare person who can translate complex concepts into simple ones. It's important to have managers in place who can articulate requirements in a way that is clear and actionable, helping to bridge gaps between people and between departments.

- *"My way" versus "your way":* Another truth is that people basically like to do things their own way, regardless of corporate standards, processes, controls, or methods. This is never going to change, but it can be controlled and mitigated.

- *Image:* For some people, the risk of looking bad is more important than risks that could cause the company to lose money or fail to find an opportunity for improvement. It takes very deliberate efforts to create an environment in which improved business performance is valued more than one's image.

- *Greed over good:* An obsessive focus on profits will never allow for the creation of a sound risk management culture. Unless they have a piece of the action, people really aren't all that excited about extraordinary profits. They care, certainly, but only to a point. And companies that have ruthlessly pursued profits at the expense of people never, ever survive. It's only a matter of time before the corporate interests are so misaligned with people's own that they start resisting—and usually in destructive ways.

- *The need to blame:* Blame is the enemy of collaboration; they always exist in reverse correlation. But there is an intrinsic human need to find the culprit. We aren't satisfied unless someone's head ends up on a stick. In truth, this is just bad management. It takes a mature organization to put more emphasis on what could be done better next time, rather than deciding who gets fired.

- *Lack of preparedness:* Given the choice, most people would rather just stick with the old standby, "We'll deal with that situation when it comes up." This is why business continuity plans are so often poorly written, untested, disparaged, and regarded as a waste of time. But the risk manager knows that responding to an event rather than planning for it is both foolish and costly.

- *Intuition:* Too many people believe that managing risk is intuitive. The more seasoned the employee, the more prevalent this view becomes. The Titanic sank because the captain's instincts told him that any iceberg big enough to sink the ship would be big enough to see. But despite having more than 30 years of experience, he was dead wrong because he had never encountered that particular scenario before.

- *The Black Swan:* The reality is that things really don't go horribly wrong very often. Odds are that, for years now, you haven't had a major security breach, your computer systems didn't melt down, you didn't have all your loans go bad, you didn't run out of cash, and your employees didn't steal all your money. But it is foolhardy to develop a certain callousness or indifference toward the possibility of such things happening.

- *Internal control mentality:* In our post-Sarbanes-Oxley[2], internal-audit-driven world, some people have the tendency to look at risk management as simply creating the right level of internal controls. But no amount of controls, no matter how numerous or comprehensive, will ever create a sound risk culture.

- *Blinders:* People's awareness of risk tends to be defined by, and largely limited to, their own area of responsibility and cognitive biases. That awareness is good, but a sound risk management culture requires that people understand a broad spectrum of risks, not just those within their own domain, and be very aware of their own biases.

- *Risk tolerances:* Like it or not, people have a tendency to set their own risk tolerances. Some want no risk (for the company or themselves) and will go to great lengths to minimize it. Others are okay playing a little fast and loose, holding to the idea that they'll just deal with things when they go wrong. Sound risk management culture means establishing and communicating a corporate risk appetite and associated policies and then taking steps to ensure that people are managing to that risk tolerance, not to what they think it should be.

- *Uniqueness:* Every person is different, each with his or her own ideas, standards, methods, values, goals, fears, failings, tolerances, skills, strengths, and biases. While this individual uniqueness would appear to be a major challenge, it can, if managed correctly, be your biggest strength.

- *Information Gaps:* Broader than Management Information Systems, information gaps relate to both known and unknown but knowable information in the hands of key risk decision-makers when they need it.

2 The Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745

SUMMARY

Culture cannot simply be summed up in one or two words. It is the collective of the personalities, values, beliefs, fears, dreams, ambitions, idiosyncrasies, priorities, and experiences of everyone in the company—and even some outside the company. It is the tone that management sets when setting the priority of working together, promoting creativity, putting egos aside, respecting one another, and—last but not least—managing risk. It is the way we do things; it is how we live our corporate life. And it takes focused, deliberate effort to make it stronger. But the reward is an environment in which people are the company's collective strength, working toward a common goal rather than individual interests.

You know you have a strong risk management culture when the following attributes are evident in your company's daily operations:

1. The board sets the right tone and expectations.

2. The CEO understands, supports, and is an advocate of risk management.

3. Everyone in the company sees risk management as a part of their responsibilities and accountabilities and raises their hand when needed.

4. Information systems and information flows support a shared understanding of risk and provide sufficient baseline for vigorous debate.

5. The company has a culture that values candor and transparency.

6. Incentive systems enforce the right behaviors, decisions, and actions.

7. A system of checks and balances is understood and welcomed.

Once you have established a sound corporate governance model with strong cultural elements, the next level of risk management involves the treatment of risk. This is largely accomplished through an effective system of internal controls and risk response.

CHAPTER THREE - CONTROL ENVIRONMENT AND RESPONSE

Let's assume your institution has articulated its business strategy and risk appetite. It has translated its risk appetite into actionable policies and created a robust risk management culture and governance system.

How can the institution be certain that risks are managed to the appropriate extent at the ground level? How do you ensure there are no unpleasant surprises?

Establishing a durable system of internal risk controls and responses helps address both of these key questions.

Having a well-defined and effective control environment is essential to managing risk in any organization, and it's also a fairly obvious objective. How to achieve this and what it means to your organization depend on many factors. This chapter reviews the common attributes of an internal control environment—specifically, how they connect and complement each other. What your internal control environment will consist of is as unique as your own organization.

INTERNAL CONTROL FRAMEWORKS

The importance of establishing and maintaining an internal control environment is reflected in the number of different control frameworks that have been adopted across multiple industries. The most commonly known is the COSO framework. In 1992, COSO (short for the Committee of Sponsoring Organizations of the Treadway Commission) issued its first publication on internal control. When the accounting debacles of Enron and Worldcom came to light in the early 2000s, the COSO framework was used as a primary example of the type of control structure an organization should have in place for ensuring the integrity and accuracy of financial reports.

With this widespread and implicit endorsement, COSO has become the default internal control framework for many organizations. It has been updated three times since its initial release, most recently in May 2013. It is certainly a sound approach and one that a financial services company can use to build its own framework.

Many of the concepts and practices described in this chapter are consistent with, if not identical to, those in the COSO framework.[3]

3 COSO is a tremendous resource that you can leverage for your institution. For more information, go to http://www.coso.org/.

DEFINING INTERNAL CONTROL

"Internal control" is frequently defined as the systems, processes, and policies that enable an organization to meet its strategic goals. An internal control framework exists to align the amount of risk assumed by the company with its accepted risk appetite and risk tolerance. However, it's not as simple as it sounds.

A good internal control environment is critical to ensuring sound operations and achieving the risk management goal of "no surprises." A truly effective and efficient internal control structure requires taking a deliberate and fundamental approach to the design, execution, and monitoring of the controls, rather than just creating them to address perceived outcomes.

Culture and attitude toward risk taking are extremely important inputs to a sound internal control environment. Understanding what your organization values, what it believes its philosophy of risk management to be, how it responds to negative events or errors, and how employees will be affected when things go wrong are all important characteristics that define what internal control means to an organization.

Is your company risk-averse or risk-loving? What does your company value more: speed to market or a fully tested product? An organization that is risk-averse may invest more time and energy in building its internal control framework, but it also needs to be knowledgeable about its ability to conduct business. Companies are paid to take risk. Without any risk, there would be no return.

Accordingly, the primary elements of an internal control environment are as follows:

- Processes and systems
- Policies
- Procedures
- Organizational structure and governance

The more nuanced elements, which are harder to quantify but no less important, include:

- Company culture and ethics
- Management philosophy
- Assignment of authority and responsibility
- Competence of personnel
- Incentives (compensation and nonmonetary)

Both the primary and nuanced elements will factor in different measures of your institution's internal control environment. Over time, this environment will evolve and take on new characteristics reflecting your culture, experience, and the impact of risk events. Some institutions will invest in their internal controls only after experiencing the negative impact of an adverse event. Others will build out a robust environment to prevent or avoid losses while running the risk of introducing potentially excessive overhead.

Most institutions, however, will fall somewhere between these two extremes. For these organizations, the internal control framework is a constant work in progress that is subject to the competitive forces related to limited resources. Let's take a look at how you might set up an internal control environment that falls into this middle category.

EXAMPLE: BUILDING AN INTERNAL CONTROL ENVIRONMENT FOR COMPANY XYZ

Company XYZ is a small but rapidly growing company looking to double in size in the next two years. Executive management and the board of directors have communicated that growth is the number-one priority and that they are willing to absorb some losses along the way in order to achieve it. As a risk manager at Company XYZ, you need to be savvy about your ERM framework and how you implement an effective internal control environment. Here are some suggested "dos and don'ts."

WHAT TO DO	WHAT NOT TO DO
• Work with the executive team to identify the most critical functions and establish a basic policy structure for daily operations. • Identify clear ownership for decision making in processes, even if the processes are not documented. • Interview the executive team to establish basic risk-tolerance levels for the most critical functions. • Find ways to use existing reports and information to assess risk levels. • Use simple techniques. • Monitor the risk-tolerance levels and provide concise reporting to executive management. • Be prepared for post-control failure analysis and accept this as part of the current culture. • Have a process in place for performing "control deficiency triage." • Be visibly, but appropriately, supportive of the executive team in its pursuit of strategy while also being willing to challenge when you assess that a critical function is at or near a risk-tolerance range. • Be prepared for more reactive risk management than proactive risk management.	• Don't roll out a complex program that requires detailed documentation and stringent rules on written procedures. • Don't try to change the strategy of the company. Highlight the risks associated with the strategy itself and in achieving it. The internal control environment exists to support your institution in achieving its goals, not to prevent it from getting there. Remember, it's about balancing risk and reward. • Don't make your internal control framework so punitive that it dis-incents management from adopting it. • Don't compromise on the critical aspects of the internal control environment that are essential to managing risk. Within the role of ERM is a responsibility to maintain risk discipline.

ESTABLISHING AN INTERNAL CONTROL FRAMEWORK: ROLES AND RESPONSIBILITIES

Now that we have a short list of the framework's elements, the next step is to establish a protocol for defining roles and responsibilities. A very common framework and one familiar to many financial services regulators is the "three lines of defense." The idea behind this concept is that the lines of business have primary responsibility for oversight of day-to-day activities and the risks associated with them. The risk management function serves as both advisor and overseer, and internal audit acts as an independent validation function.

All three lines of defense are managing risk on a daily basis, but they do so within the context of their assigned roles. It is up to executive management, in coordination with the risk committee and the board of directors, to establish the roles for managing risk, to develop the strategic plan, and to set the risk appetite and tolerance levels within the context of the strategy. Once these have been established, it is up to the management within the three lines of defense to execute the strategy and manage the institution within the risk appetite and risk-tolerance guidelines.

FIRST LINE OF DEFENSE: THE BUSINESS UNITS

- Owns the risk.
- Is held accountable for risk identification and escalation.
- Manages risk (for example, in the case of credit risk, by selecting and evaluating customers, structuring transactions, obtaining approvals, and escalating issues based on portfolio monitoring).

The lines of business—or, in this context, the first line of defense—manage the day-to-day processes of the institution. These groups are the process and risk owners, and they are expected to monitor activities, respond to and report on unexpected events, and ensure that all activities are conducted within the established risk parameters. Their mandate also includes performing periodic assessments to identify additional risks and implement any supplementary measures to mitigate those risks. They are also responsible for designing and implementing control-level policies and procedures, as well as escalation procedures for responding to significant events.

The first line of defense not only is accountable for primary risk mitigation, but is also rewarded for revenue generation and growth of the institution. Typically, these risk takers are rewarded through compensation plans that incentivize them to meet revenue and growth goals. It is essential to include controls and governance on incentive compensation in your institution's internal control environment. That way, you ensure that properly balanced incentives include recognition of the first line of defense's role in managing growth as well as risk.

SECOND LINE OF DEFENSE: RISK MANAGEMENT, FINANCE, COMPLIANCE, AND OTHER CONTROL GROUPS

- Establishes the risk management framework.
- Ensures that the first line of defense's activities accord with risk appetite and risk tolerance.
- Establishes policy and credit underwriting guidelines.
- Monitors portfolio quality and concentrations and also manages problem credits.

The risk management group plays an important role as the second line of defense, supporting management in identifying, assessing, and mitigating risk. It is worth noting that risk management functions will look different in small institutions than larger ones, and the roles will shift as the institution grows. In small institutions, where there may not even be a Chief Risk Officer let alone a risk management group, this role will often be shared by executive management. However, even in an institution without a designated, full-time CRO, the institution should still designate someone as the primary driver of the risk management program, particularly as it relates to designing enterprise risk assessments, risk reporting, and event response.

At the other extreme, for large institutions it is fairly common to have a centralized (corporate) risk group that is independent of management. This group is responsible for risk oversight and management support, but it does not have day-to-day involvement with operations. Complementing this group will be risk managers who are embedded throughout the organization and, at an operating level, serve as stewards of the risk management program. There may even be a CRO designated for one or more operating units. Unlike the corporate risk group, these risk managers participate in business unit risk assessments, reporting, and the first line of defense's control testing.

Regardless of which model your institution currently uses, it is assumed there is at least one person in charge of driving the design and implementation of the ERM risk assessment framework. Implementation of this framework includes developing management and executive-level risk reports and participating in risk oversight (that is, risk measurement, monitoring, and testing). For either the individual risk officer or a corporate risk group, it is critical that these roles be kept separate from the lines of business. In order to provide effective oversight, the risk management function needs to have independence from operations and be in a position to challenge authority over day-to-day operations.

The risk management function should also assist and provide input into ongoing risk assessments and have the authority to challenge those assessments. The risk reporting developed between the business units and risk management assists in creating transparency around key processes and risk acceptance and should include views from both the first and second lines of defense, particularly when there is disagreement over the level of risk that exists.

THIRD LINE OF DEFENSE: INTERNAL AUDIT AND CREDIT REVIEW

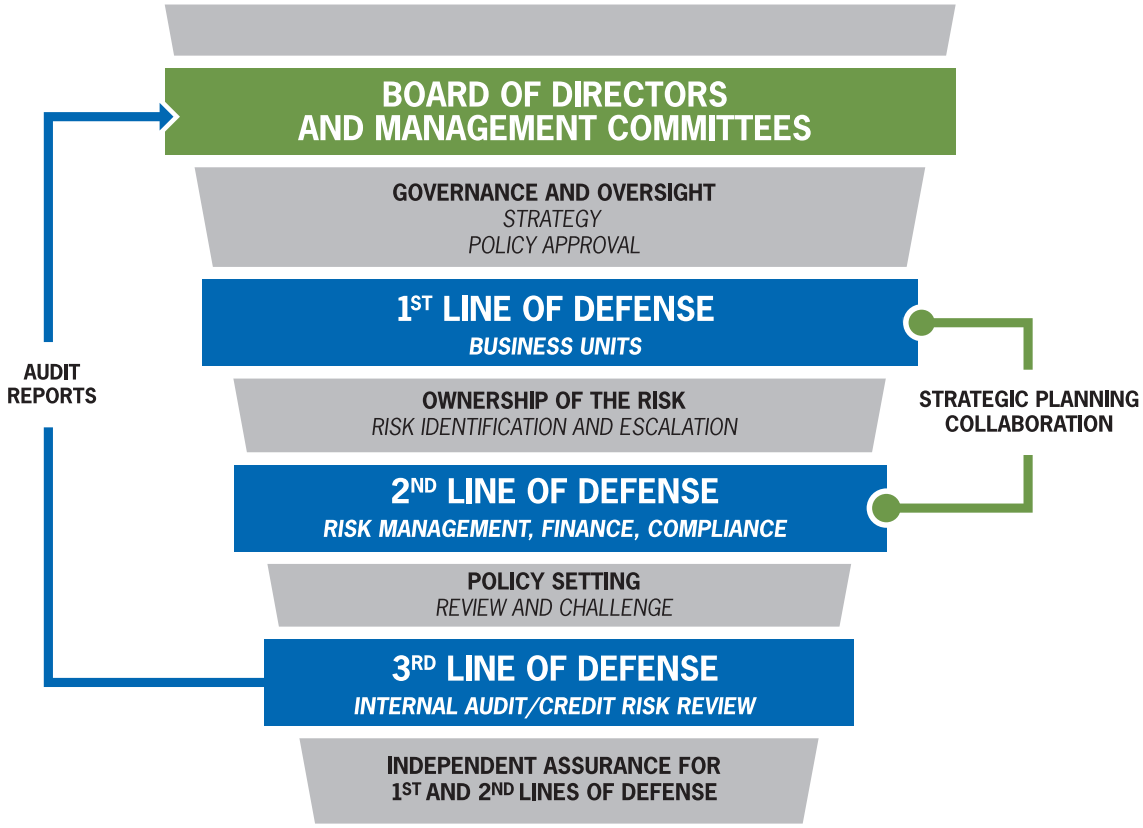
- Internal audit provides independent review of the bank's activities.

This is the third and final line of defense for credit underwriting and ensuring effectiveness of the risk framework. Internal audit provides assurance to the audit committee, board of directors, and management that the organization's operations and related internal controls are working effectively. Typically, internal audit uses a risk-based approach that is developed independently from management's assessment. Discrepancies between internal audit's risk assessments and management's ERM assessments should be discussed and the differences resolved at the outset of any audit.

In too many organizations, the emphasis has been on the question, "Is the control being performed?" But it would be more meaningful to ask, "Is the control effectively reducing the risk to an acceptable level?" While the first issue is essential—a control that isn't being performed will not be effective—taking the next step and examining whether the control is performing as intended and operating to mitigate the risk is where internal audit plays a key role in the internal control framework. Periodic testing across the company by competent internal auditors is a critical component and provides a healthy tension that makes the entire internal control framework effective.

For many institutions, loan review or credit risk review also falls within the third line of defense. When an institution has both audit and risk committees of the board, credit review will report independently to the latter.

Collectively, the three lines of defense provide a multipronged approach to ensuring that risk isn't just managed, but that it is aligned to what is acceptable and expected in pursuit of a given return.



A SUCCESSFUL INTERNAL CONTROL FRAMEWORK

With clear roles established and high-level responsibilities assigned to the three lines of defense, we can now look at the "nuts and bolts" of building an internal control framework.

Let's start with the basics of processes and controls. In order to achieve our strategic objectives, we develop processes. Within the design of those processes are certain assumptions about how the process will work and what the expected outcome will be. However, there also exists a range of alternative outcomes, some of which may be better than expected (for example, favorable market conditions, project costs lower than expected, etc.), as well as undesirable outcomes (such as process breakdowns, unexpected costs, security incidents, vendor failures, fraud, etc.). Consider the processes that make up day-to-day operations and their possible outcomes, and then set out to build control systems to minimize the likelihood that these negative outcomes will occur.

CONTROLS

Understanding the nature and types of controls that you have within your process is an important step to understanding the strength of your overall design and evaluating the controls that are in place. Let's work with the most fundamental control types.

There are many different types of controls, but almost all of them can be characterized along two dimensions: their placement in the process and how the control is initiated. If a control is a precursor to an outcome or limits the type of outcome, it is a *preventive control*. If a control is placed after the process step is complete and it is verifying an outcome, then it is a *detective control*.

Control initiation is similarly intuitive. A control that is initiated by a system or that occurs without intervention by a person is considered an *automated control*, whereas a human-based control is a *manual control*.

Understanding the nature of your controls is essential in evaluating the strength of your internal control environment's design. You could have a process with multiple controls, but if they are all occurring post-processing and are all manually initiated, then the design of your control environment lends itself to more post-event risks.

Determining which type of control to use will depend on many factors, including the following:

- *Nature of the process:* If the process is highly automated, you may be able to leverage technology and implement automated controls.

- *Type of risk:* Some risks are easily detected and can be mitigated through straightforward controls. Others manifest or emerge only after the completion of a transaction or process. For example, an ATM machine has a control for unauthorized access to an account: the use of a personal identification number (PIN). The PIN is an example of an automated, preventive control. But what happens if someone has both the card and the PIN? Other controls designed to detect fraud, such as monitoring spending or withdrawal history, may trigger an alert and flag an account for potential fraudulent activity.

- *Size of risk:* While no institution wants to have any risk, mitigation of *all* risk is unachievable. Not only is such mitigation costly, but it can thwart human creativity, which is evolving all the time. Your control environment should be "right sized" to the level of potential risk.

When building an internal control environment, avoid building a $10 fence for a $5 dog.

POLICIES AND PROCEDURES: THE FOUNDATION

Every company possesses policies and procedures in some degree or form, but how are they used? How effective are they? What purpose do they serve? All organizations should be asking these questions as they build and refine their internal control environment.

POLICIES

Policies are the documents that set the tone of a control environment. They serve as the fundamental set of rules that govern how business is to be conducted. They form the boundaries for risk management and make it clear that it is management's responsibility to see that risk is managed within those boundaries.

Policies can exist across the organizational structure. For our purposes, let's look at the differences and similarities between board policies and operating policies.

- *Board policies* (also known as bank policies, corporate policies, etc.) express the company's risk appetite to the masses and provide institution-wide guidance and risk expectations. While they may largely impact only one part of the institution, they apply to everyone. Examples include the corporate risk management policy, credit policy, liquidity policy, and information security policy, among others. These policies are ratified by the board (or a designated committee of the board) at prescribed intervals, with an annual review being most common.

- *Management or Operating policies* are typically more operational or technical in nature, and they usually apply only to a specific operating area of the institution. Examples may include policies related to technology systems, technical compliance requirements, or other department-specific policies. These policies are usually owned and updated by a specific department and are typically ratified by the bank's risk committee or some other governing body.

Regardless of the type of policy, your institution should have a specific process for developing, approving, and maintaining policies that are widely communicated and that include expectations of adherence.

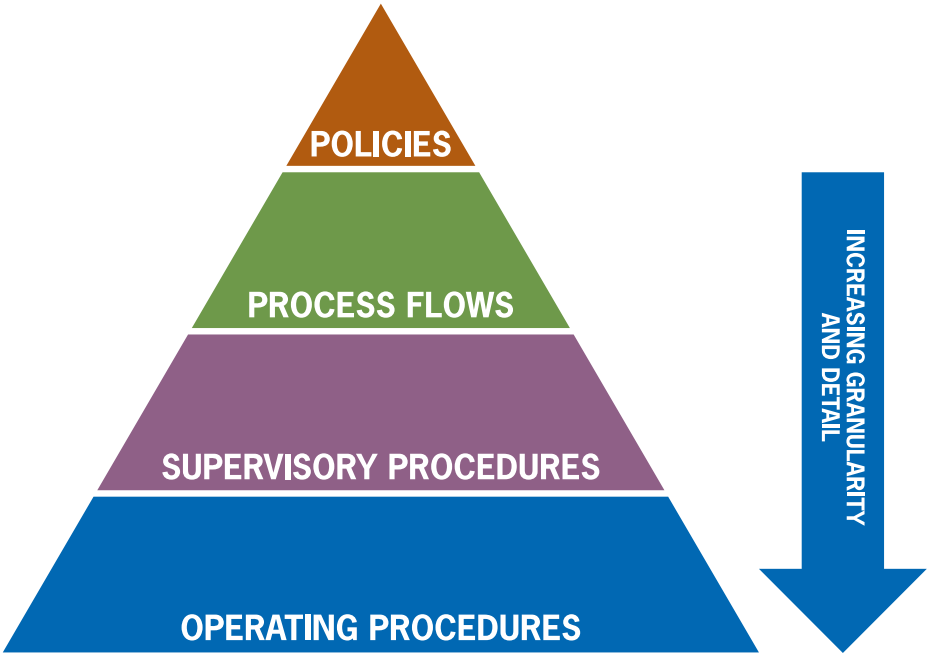
PROCESS FLOWS

Process flows, supported by supervisory and operating procedures, 1) capture the essentials of how a process progresses from a starting point (where hand-offs between departments occur), 2) specify which systems are critical in performing a crucial step, and 3) identify control points along the way.

Process flows are becoming more and more essential to an internal control environment, given the need to communicate to external parties how the institution's critical functions are executed. They are, however, another piece of documentation that requires ongoing maintenance. If you plan to include process flows in your internal control documentation, be sure you have identified the ongoing maintenance requirements needed to support their upkeep and to maintain their consistency with your policies and procedures. Thought should be given to the process flows that have already been constructed for Sarbanes-Oxley controls and reusing them for risk management purposes.

PROCEDURES: OPERATING AND SUPERVISORY

Procedures are commonly used control tools. How you approach them at your institution should be consistent with your size, complexity, and ability to maintain them. Operating procedures should describe the "how to" of a process at the most granular level. Granular in this context is defined as the level of detail the institution wants to capture. For some organizations, this may be step-by-step instructions detailing the mechanics of a process. For others, it may be a more general description of how a process is accomplished. Regardless of the level of detail, you should have some standards established to drive a certain level of consistency across the institution's documentation.

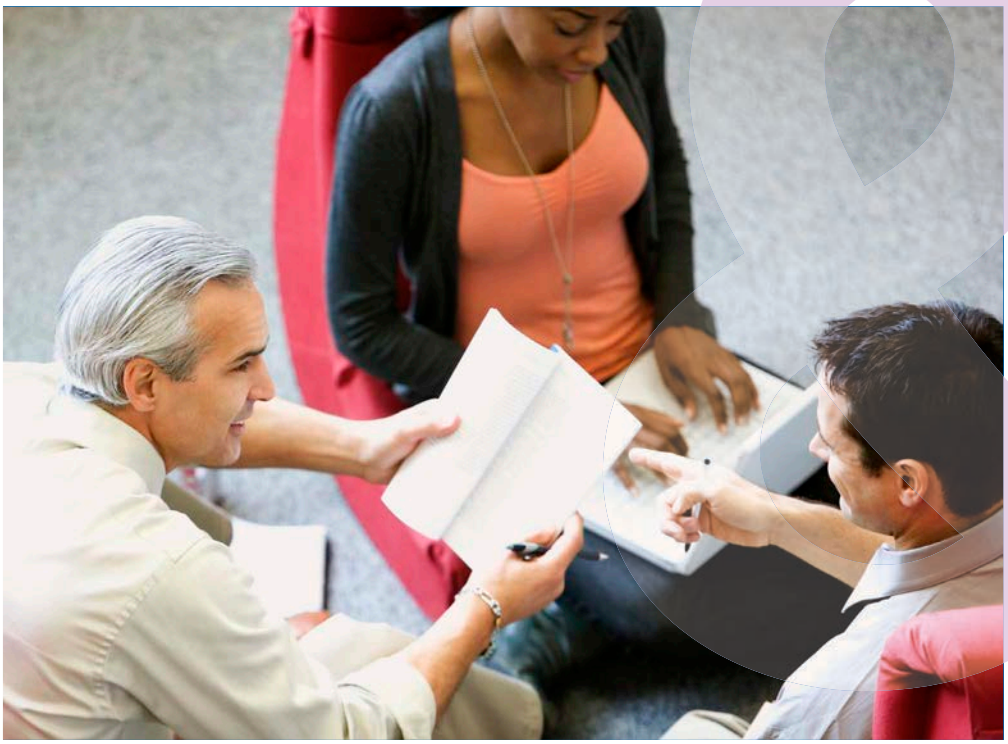


ASSESSING YOUR INTERNAL CONTROL ENVIRONMENT

Once the processes and controls are in place and operating, the next step is to establish a framework for assessing the effectiveness of the risk-mitigating controls. Remember, the first line of defense owns these processes and is accountable for managing them and ensuring they operate within an acceptable risk tolerance. The second line of defense needs to ensure that the first line is living up to this expectation. This is an area where ERM has a crucial role.

The ERM program is instrumental in establishing how these assessments are conducted. Regardless of structure, it is essential to the internal control environment to have a mechanism for assessing the risk to the institution, based on a range of plausible scenarios and the strength of the institution's controls in managing that risk. The value for the business—the first line of defense—is that, in addition to being active risk management partners, the ERM capabilities and its assessments can also serve as the basis for developing strategy and new products.

There are several methods for assessing your internal control environment. A robust environment will use more than one, and potentially all, of the following methods for a given process.



ASSESSMENT TOOL	PROS	CONS
1. *Self-assessments and internal risk surveys:* A process by which business unit managers attest to the design and effectiveness of the processes and controls under their supervision.	1) Cost-effective; 2) attestation is closely linked to the accountable owner of the control.	Attestation is not independent. A risk of bias may result in your control environment being rated stronger than it actually is.
2. *Scenario analysis:* Periodic exercises that involve key business leaders, stakeholders, and risk managers in identifying and sizing the risk posed to an institution under plausible scenarios.	1) Offers a comprehensive, transversal view of institution; 2) involves a broad range of participants with multifaceted views of risk; 3) includes external experience from other institutions.	1) Is time-intensive (requires dialogue and active meeting participation); 2) tends to focus on events or large risk types; could miss more routine risk events; 3) relies on multiple assumptions.
3. *Control testing:* Testing can occur in all three lines of defense, but have different objectives. Control testing performed by internal audit is typically considered the most reliable, given this group's independence from the business line.	1) Is readily understood by everyone; 2) reinforces the need for evidence of control execution.	1) Control testing is time-intensive and requires dedicated individuals; 2) not all processes are suited to validation by control testing. Processes that are executed infrequently typically are best assessed by control testing.
4. *Control failure analysis (or lessons learned):* Using the opportunity when something goes wrong to explore the root causes of the failure and to make systemic changes to your control environment based on the analysis.	1) Offers the opportunity to learn from mistakes made; 2) raises awareness and builds risk management culture.	Is reactive to a risk event and doesn't have a component to assess risk before a problem occurs.

In addition, part of what a well-structured ERM assessment should do is consider a range of risk types as a way to thoroughly understand the impact of alternative outcomes. Although in considering any possible outcome the emphasis is on the overall possibility of a process failure, the analysis can bring benefits through discussions that consider the different types of risk (credit, liquidity, operational, etc.). We don't manage risk within these risk silos, but by considering them we gain a richer understanding of the risk embedded in these scenarios and their potential impact on the institution.

Key controls can be regularly evaluated and tested, both by the owner and by independent sources, typically internal audit. Business units should not be surprised to be held accountable for their control environments and should be expected to certify their risks and controls at some interval (quarterly or annually), as well as issue statements about the residual risk profile. In turn, the oversight functions, such as risk management and internal audit, are also accountable for challenging these self-assessments if they seem inconsistent with historical experience, industry norms, or even common sense.

It is not uncommon for individuals responsible for a business process to be too close to it to see vulnerabilities that are readily apparent to a trained risk manager. Reiterating the earlier point, having clear roles and responsibilities identified up front will reduce friction when your first line of defense—the business process owners—knows that the second and third lines of defense have the power to effectively challenge their ratings.

Finally, it is critical to understand that the assessment of the internal control environment is relevant only within the context of risk tolerance. To conduct an assessment without the benefit of first establishing risk appetite, and risk tolerance, is an analysis that has no context. People need to know what to do with this information and whether the analysis shows risk to be within, or outside of, acceptable limits.

WHEN CONTROLS BREAK

Having good controls in place is the first step in managing risk to an acceptable level, but control design is only the beginning. In order for a system of controls to work effectively, it must be combined with systems for monitoring activities and identifying when activities take place that either violate a control or indicate a potential risk despite the presence of a control.

For any given process, there are an almost infinite number of ways that things can go differently from expectations, and no scenario analysis, no matter how exhaustive, can uncover all conceivable scenarios. Therefore, it is incumbent on management to ensure the existence of suitable event-monitoring mechanisms and clearly defined processes for responding when things don't go right.

When evaluating issues that do arise, it is important for management to stay focused on understanding the impact of the event, its root causes, what needs to be done to recover from the event, and what can be done to prevent it from happening again. Unfortunately, too much time can be spent figuring out which person to blame, but this is informative only within the context of corrective actions. In fact, if someone does cause an error or problem, then this person should be given the first chance to suggest ways to improve the process so that the incident can be avoided in the future.

For large incidents, every institution should have some form of reporting mechanism to the governance committees for presenting and discussing issue identification and resolution. Learning does not stop at the department level, and if senior management and the board are going to be part of the process of managing risk tolerance, they must be made aware of what is happening within the organization. Again, the emphasis should always be on, "What happened, what does it mean, and what are we doing about it?" To the extent possible, balance the need to attach accountability to specific individuals with the desire to have a culture that encourages these same individuals to come forward *before* an issue arises. Creating a culture that exacts punishment when a control failure occurs will only encourage others to hide their potential weaknesses.

That said, repeat issues or findings of repeat control weaknesses are dealt with differently depending on the number of people they involve. If the root cause consistently lies with one person, then this is an HR issue. But if it is an issue of poor process design, under-developed or ineffective controls, or actions outside of one's control or the result of changing circumstances, then these must be dealt with at a process and control design level. If you make people afraid to point out weaknesses for fear of criticism, you will never achieve a mature risk management state. All employees should have the ability to challenge—without recrimination—assessments or assumptions related to any process or control.

Finally, the value of instituting a process for control failure analysis will be obvious when the inevitable happens and some unexpected event needs review. The process should include the following steps:

1. *Re-analyzing the base risk assessment and related internal controls.* Did the event provide any different perspective on the inherent or residual risk? Do you still feel that the residual risk is within acceptable tolerance levels?

2. *Evaluating the controls.* Are the related controls too weak? Too rigid?

3. *Reviewing policies and procedures.* Are adjustments warranted to policies, processes, or even people?

Building a sustainable risk management program requires building in self-teaching mechanisms. This requires a level of honesty and transparency that doesn't always exist. It is a mature organization that can move past individuals and focus on strengthening the institution.

RISK MONITORING AND REPORTING

The nature of risk management programs is that they create a lot of information. The key is to figure out which information is truly meaningful and actionable. Risk reports shouldn't create paper—they should create dialogue.

A prerequisite for effective risk monitoring and reporting is a culture that rewards learning, encourages transparency, demands cooperation, and punishes fortress mentality.

Here are some important points to remember:

- Risk reporting is only as good as the level of honesty and transparency that is allowed.
- Any report that doesn't say something specific about where the institution is going and what it is doing isn't worth much.
- Information reported without context can be extremely dangerous.
- The report doesn't have to be the same one every month.
- Good risk reporting has to say something about macro risks and micro risks.
- Risk does not happen in types, but in processes.
- Ask if your risk reports say anything about whether an operation is aligned with the institution's risk appetite.

SUMMARY: KEYS TO A SOUND INTERNAL CONTROL ENVIRONMENT

Creating and sustaining the appropriate internal control environment is a journey, not a destination. Organizations are constantly changing. They are exposed to new and different risks. They are impacted by their leadership and the strength of the governance process, along with a myriad of factors that will pose a constant challenge. Despite these challenges, some pitfalls are avoidable as you build out your internal control environment. Take these points into account as you embark on your journey:

- *Emphasize quality, not quantity.* The number of controls you have in a process is less important than the quality of those controls. A well-designed control that is placed appropriately within a process can garner a lot of "bang for the buck."

- *Find a way to quantify the perception of risk.* Sometimes something just "feels" risky, so we create systems to theoretically reduce that risk. While this perception may in fact be based on experience and sound judgment, it is, at the end of the day, still a perception. Consistently apply a method for risk quantification so that you don't find yourself exposed to a real risk that was outside of your perception.

- *Remember that context matters.* A control lacking context, or a control without clearly documented assumptions about the nature of the risk being mitigated or about the expected residual risk level you are aiming for, is a control that will not be effective.

- *Maintain and reward transparency.* This is as much about your culture as it is about process. If your residual risk level lacks transparency (out of fear that communicating this risk will somehow be perceived as a control weakness), this works against the objective of the process. Regardless of the level of controls and the transparency around it, the risk still exists!

- *Keep controls relevant.* An overemphasis on whether or not the control is being maintained, rather than a broader discussion about the purpose of the control and its true effectiveness, will diminish the effectiveness of the internal control framework.

- *Keep a healthy balance between process and judgement.* Regardless of how many controls are in place, people still need to use their heads. A good control structure should provide for a certain number of specific steps while allowing for some flexibility in execution (subject to the underlying risks involved).

An institution with a strong risk culture and risk management program is further strengthened by having a reliable and sustainable internal control environment. This environment enables an institution to effectively manage its processes, allows visibility into its strengths and weaknesses, and supports its ongoing soundness.

CONCLUSION

Having the right risk management governance, culture, and internal control environment is about controlling what can be controlled. These concepts are not new. Companies in the financial services industry have always been expected to know the risks they face and to manage them appropriately. Articulation of risk appetite, policies and procedures, governance, internal controls, risk measurement, data infrastructure, reporting, and all the other risk management activities are mission critical but of dubious value if the company does not have the right culture.

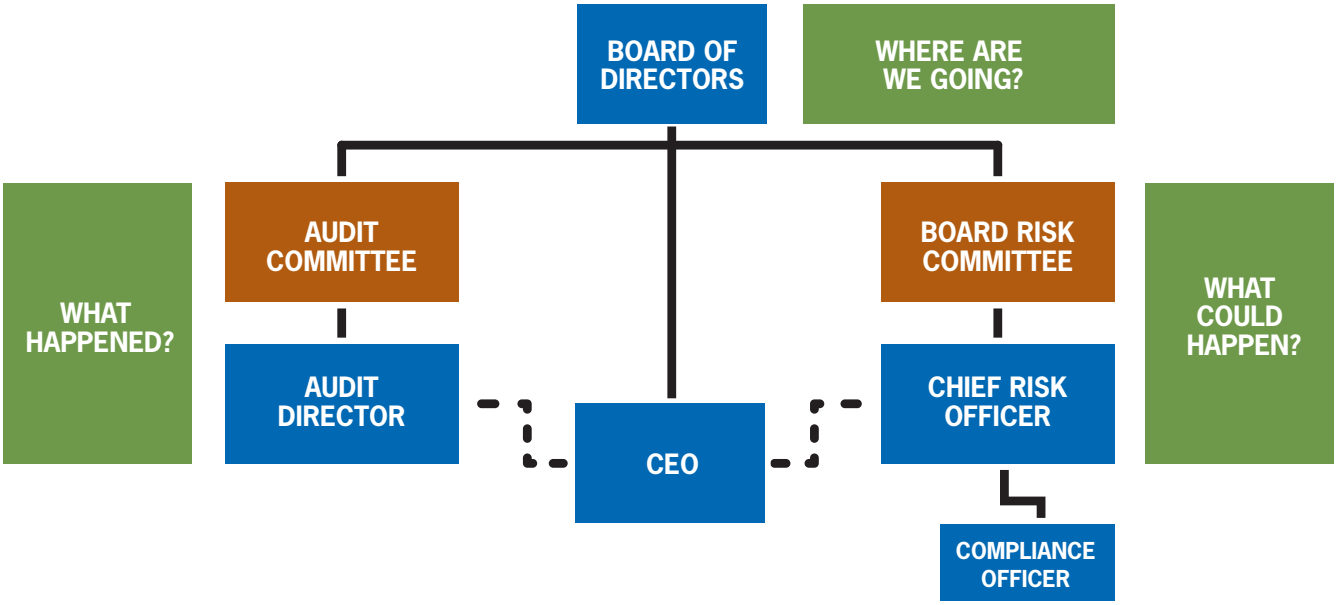
Risk management culture can be the single most important element that guides a financial institution through economic cycles. Along with sound risk management and solid, well-developed business strategies and capital plans, a healthy risk culture contributes to success. Banks that continually improve on these elements have a competitive advantage.

Strong financial institutions realize that the goal is not to avoid risk but to ensure that the risks are understood, and that they can earn an appropriate return for accepting and managing them[4].

4 Remarks by Carolyn G. DuChene, Deputy Comptroller for Operational Risk, before the American Bankers Association Risk Management Forum, April 25, 2013.

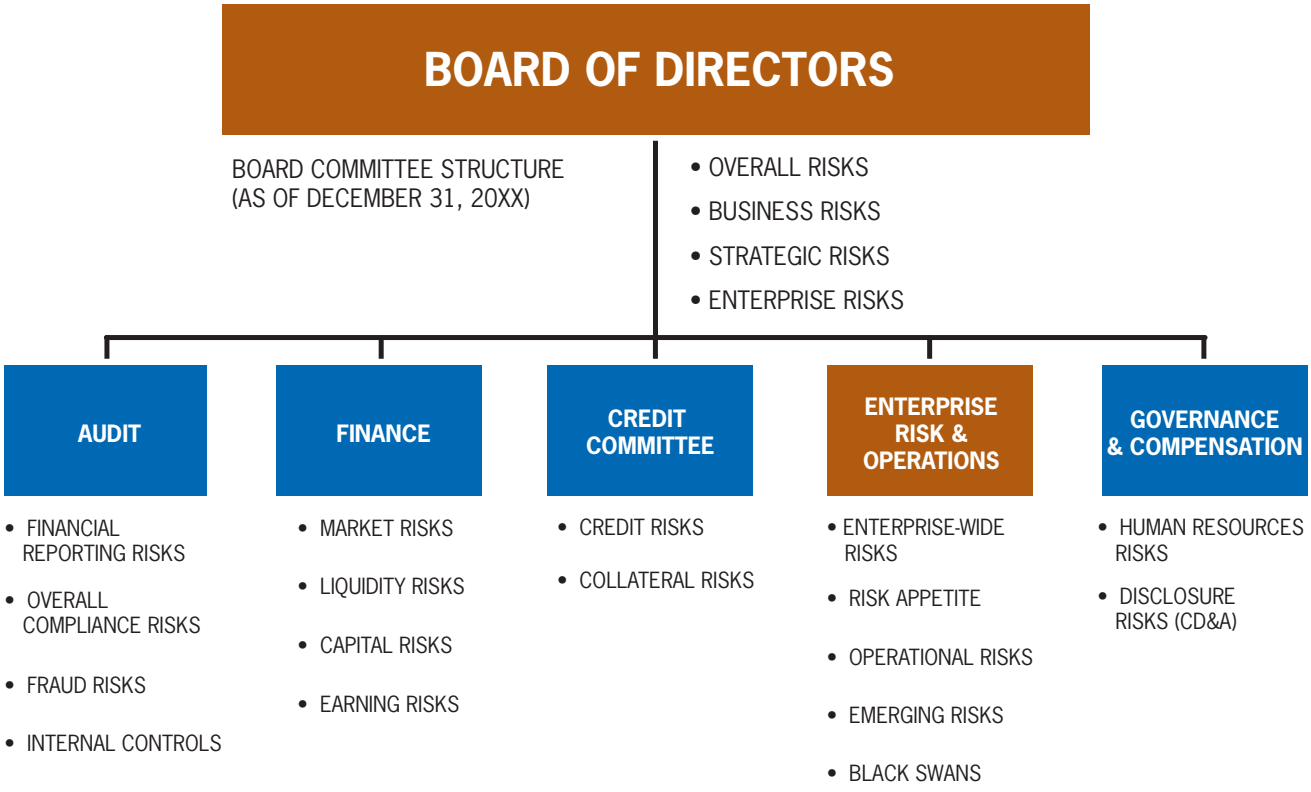
APPENDIX A - BOARD-LEVEL COMMITTEE STRUCTURE

APPENDIX A
BOARD-LEVEL COMMITTEE STRUCTURE - EXAMPLE 1



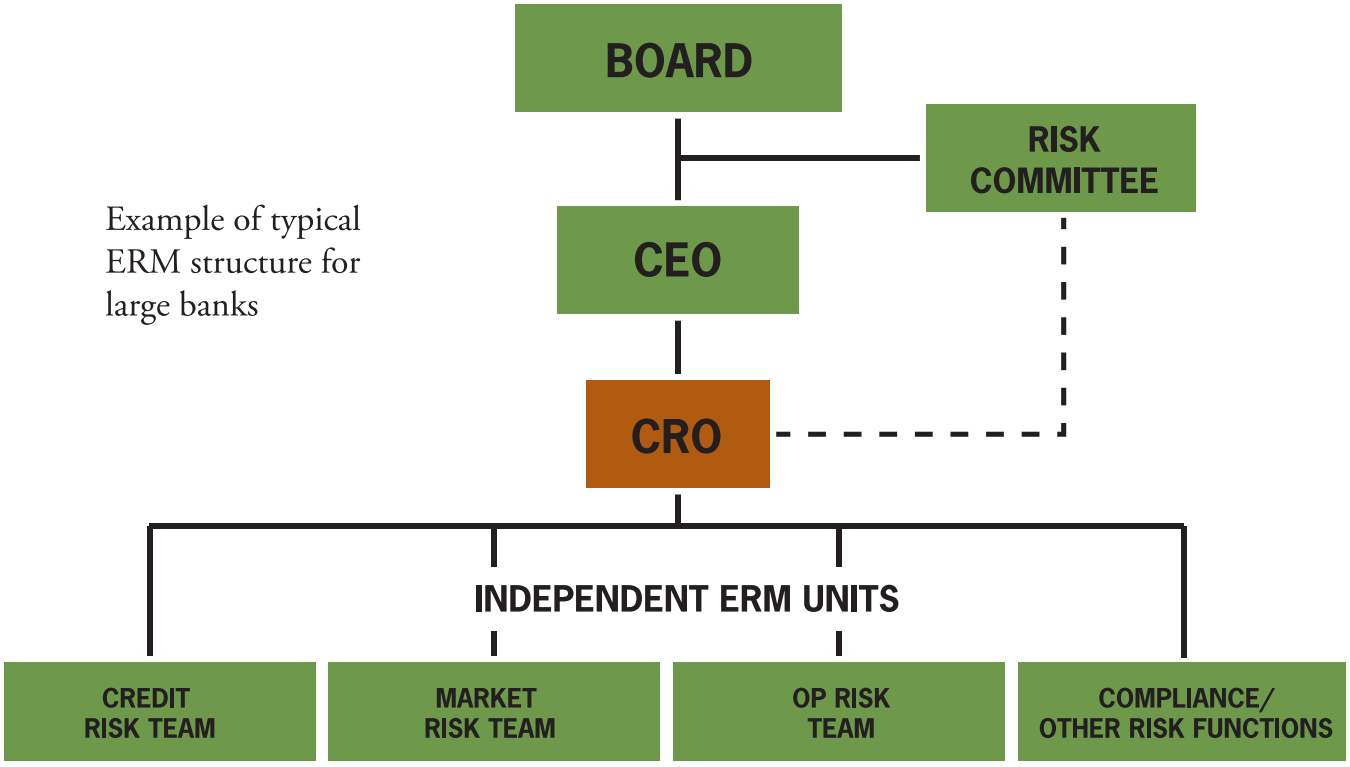
BOARD COMMITTEE STRUCTURE - EXAMPLE 2

The purpose of the enterprise risk and operations committee of the board of directors is to advise and assist the board with respect to enterprise risk management, operational risk, information technology, and other related manners.

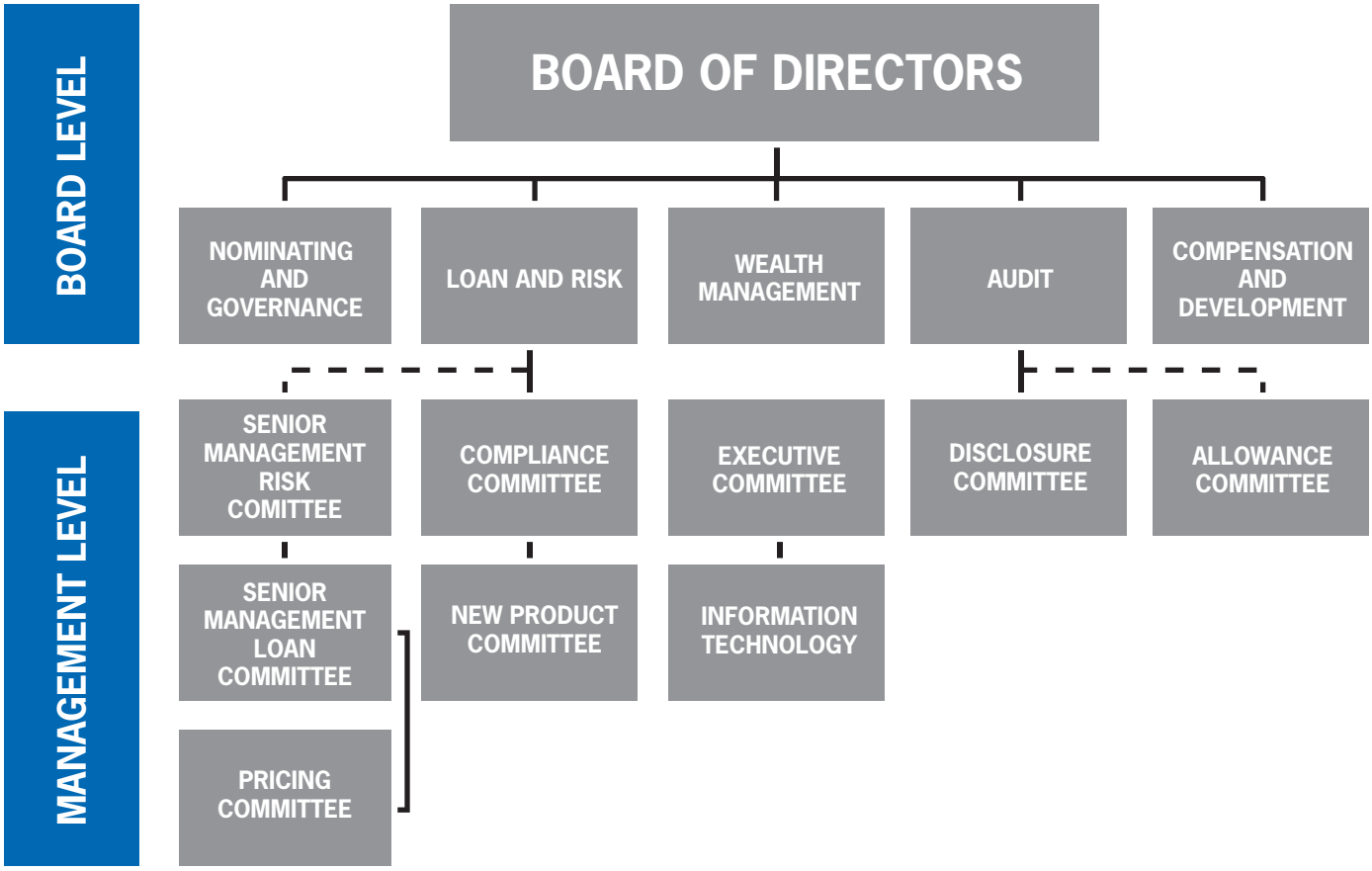


BUILDING THE RIGHT ERM STRUCTURE/TEAM - EXAMPLE 3

Example of typical ERM structure for large banks



EXAMPLE 4



WHO SHOULD DO WHAT?

BOARD OF DIRECTORS	SENIOR MANAGEMENT	RISK MANAGEMENT
• Approval of policies • Approval of key documents (Risk Appetite, Strategic Plan, and Capital Plan) • Approval of key reports to determine adherence to policies and key documents • Hold senior management accountable • Approve board risk management "charter/ mandate" • Approve enterprise risk management (ERM) "mandate"	• Provide regular reports to the Board or its committees that reflect status of adherence to risk levels. • Communicate to employees on a regular basis the risk culture and appetite of the bank. – Senior management staff meetings – ERM – Business lines – Audit – Compliance • Hold employees accountable for actions when they step outside of the risk culture and appetite • Ensure accurate and timely information to make informed decisions • Ensure adequate and qualified staff to manage and oversee risk of the company.	• Develop ERM mandate • Develop appropriate and timely reporting of key risks metrics (board and senior management) • Conduct key communications with: – ERM staff – Business lines – Human Resources

APPENDIX B - BOARD-LEVEL RISK COMMITTEE CHARTER

COMPOSITION AND INDEPENDENCE, EXPERIENCE, AND AUTHORITY

The risk committee will be composed of members of the board of directors in such number as is determined by the board with regard to the by-laws of the bank, applicable laws, rules and regulations, and any other relevant consideration.

The members of the committee will be appointed by the board and will serve until their successors are appointed.

A chair will be appointed by the board upon recommendation of the corporate governance committee; otherwise, members of the committee may designate a chair by majority vote.

The committee may from time to time delegate to its chair certain powers or responsibilities that the committee itself may have.

Committee members may enhance their familiarity with risk management issues by participating in educational programs conducted by the bank or an outside consultant.

In fulfilling the responsibilities set out in this charter, the committee has the authority to conduct any investigation and access any officer, employee, or agent of the bank appropriate to fulfilling its responsibilities, including, without limitation, the shareholders' auditor.

MEETINGS

- The committee will meet at least XXXX times annually, or more frequently as circumstances dictate.

- The committee will meet separately with the bank's Chief Risk Officer (executive session) at each regularly scheduled meeting, and with other selected members of management as considered necessary by the committee, to discuss any matters the committee believes should be discussed privately.

- Risk committee members should also have representation on the audit committee.

SPECIFIC DUTIES AND RESPONSIBILITIES

To fulfill its responsibilities and duties, the committee will satisfy itself that sound policies, procedures, and practices are implemented for the management of key risks under the bank's risk framework, which includes market, operational, liquidity, credit, insurance, regulatory, legal, and reputational risk. More specifically, the committee will:

- Review and approve the bank's risk appetite statement and risk appetite governance framework at least annually and on the recommendation of the Chief Risk Officer.

- Review the bank's actual risk profile against its risk appetite, as well as any exceptions to risk appetite metrics as reported by senior management.

- Review risk management's annual assessment of the bank's performance against the enterprise risk appetite statement.

- Meet annually with the human resources committee (HRC) to review the risk input into compensation decisions, prior to the HRC determining year-end incentive compensation.

- Receive presentations and other information to understand the significant and emerging risks to which the bank is exposed. This includes reviewing on an annual basis management's report on enterprise-wide stress-testing results and identifying material risks and emerging risk issues and trends.

- Review with management the bank's policies and procedures on risk identification and monitoring, including emerging risk identification.

- Approve, where appropriate, policies developed and implemented to measure the bank's risk exposures and to identify, evaluate, and manage the significant risks to which the bank is exposed. Such policies and procedures should be reviewed at least once a year to ensure they remain appropriate and prudent.

- Oversee significant new initiatives (potential acquisitions, new locations, new products and services, etc.) from the point that they are proposed, ensuring that the incremental risk profile is consistent with stated risk appetite and overall business strategy.

APPENDIX C - JOB DESCRIPTION FOR CHIEF RISK OFFICER

Level: Senior Executive

Reporting: <Board risk committee or CEO>

Responsibilities

The Chief Risk Officer (CRO) serves as a key member of the <*company name*>'s executive management team and is responsible for the design, communication, implementation, and oversight of <*company's*> enterprise-wide risk management policy, program, and framework. Specific responsibilities include the following:

- Serves as chair for management's risk committee
- Ensures that an enterprise-wide risk management (ERM) framework is in place that follows industry best practices in the identification, assessment, and mitigation of risk
- Assists the board and senior management in communicating that framework within the organization, including the goals and objectives of the ERM program
- Assists the board and senior management in integrating risk management practices into strategic planning, bank operations, and change-management
- Assists the board and senior management in developing a process and structure for defining and communicating risk appetite in the pursuit of fulfilling strategic objectives
- Assists the board and senior management in developing appropriate risk management policies
- Ensures that management has developed suitable risk classifications
- Assists management as needed in developing and updating enterprise risk assessments

- Assists senior management in ensuring that suitable risk-mitigation controls are in place for all key risks and that risk-monitoring systems are developed and maintained

- Develops a reporting framework that allows for the aggregation of enterprise-wide risk profiles and assessment information, to be presented to the board and risk management committee for review and action as needed

- Ensures that management systems are in place to oversee compliance with all policies and applicable laws and regulations, including a process for responding to policy exceptions and violations

- Ensures integration between the ERM framework and internal audit's program

- Conducts management training as needed on risk management practices and procedures

- Serves as subject-matter expert to the board and senior management in the risk aspects of strategic planning, risk alignment, capital management, resource planning, new projects and services, risk reporting, and regulatory compliance

Optional responsibilities where appropriate or desired:

- Serves on the board's risk committee (if one exists)

- Supervises other oversight roles, such as the Chief Compliance Officer and the Chief Information Security Officer

- Oversees compliance with and validation of Sarbanes-Oxley requirements

APPENDIX D - SUGGESTIONS FOR FURTHER READING

Robert A. Prentice and Yousef A. Valine, "Don't Kid Yourself, You're Biased," *The RMA Journal®*, July–August 2013.

Edward P. Schreiber, "Enterprise Risk Management – Governance and Policies," *The RMA Journal®*, June 2012.

Yousef A. Valine, "Establishing Enterprise Risk Management Competencies," *The RMA Journal®*, April 2012.

Malcolm D. Griggs, "From Your RMA Leadership – Good Governance versus Effective Governance," *The RMA Journal®*, March 2010.

Nicholas Hayes, "Governance for Strengthened Risk Management," *The RMA Journal®*, May 2013.

Henry Killackey, "Integrating Enterprise Risk Management with Organizational Strategy," *The RMA Journal®*, May 2009.

Bill Githens, "From Your RMA Leadership – Risk Culture is the Bedrock of a Robust ERM Program," *The RMA Journal®*, April 2011.

Dick Evans, "Strong Culture Guides Sound Risk Management," *The RMA Journal®*, February 2013.

M. Robert Rose, "The Nature of a Balanced and Embedded Risk Culture," *The RMA Journal®*, July-August 2013.

Jack Wixted, "From Your RMA Leadership - Top 10 Attributes of a Best-in-Class Risk Management Culture," *The RMA Journal®*, July-August 2012.

Bill Githens, "From Your RMA Leadership - Your Bank Culture Is at the Center of Your Success," *The RMA Journal®*, November 2012.