ima®

The Association of Accountants and Financial Professionals in Business

Implementing an Effective Risk Appetite

Statement on Management Accounting

About IMA®

IMA, the association of accountants and financial professionals in business, is one of the largest and most respected associations focused exclusively on advancing the management accounting profession.

Globally, IMA supports the profession through research, the CMA® (Certified Management Accountant) program, continuing education, networking, and advocacy of the highest ethical business practices. IMA has a global network of more than 75,000 members in 120 countries and 300 professional and student chapters. Headquartered in Montvale, N.J., IMA provides localized services through its four global regions: The Americas, Asia/Pacific, Europe, and Middle East/Africa. For more information about IMA, please visit **www.imanet.org**.

About the Author

James Lam

Lam is president of James Lam & Associates, a risk management consulting firm he founded in 2002. He works with corporate directors and executives of large, complex organizations including financial institutions, energy firms, multinational corporations, regulatory agencies, and nonprofits. In a Euromoney survey, Lam was nominated by clients and peers as one of the world's leading risk consultants.

Institute of Management Accountants
10 Paragon Drive, Suite 1
Montvale, NJ, 07645
www.imanet.org/thought_leadership

Research Area

Statement on Management Accounting

SMAs present IMA's position on best practices in management accounting. These authoritative monographs cover the broad range of issues encountered in practice.

Topical Area

Risk Management and Internal Controls

This research area focuses on frameworks, methodologies, and approaches used by organizations to understand the risks they are exposed to, put controls in place to counter threats, and effectively pursue their objectives.

Executive Summary

If strategy is doing the right things whereas operations is doing things right, then risk management is the capability of doing both effectively under uncertainty. Organizations face uncertainty in many forms. In addition to strategic and operational risks, they face financial, legal/compliance, and reputational risks. Enterprise risk management (ERM) is a global, widely accepted approach to identifying, assessing, measuring, and managing the key risks faced by an organization, including the critical interdependencies between the risks.[1]

During the global financial crisis of 2008, many companies around the world were caught off guard by unknown risks or under-reported risk exposures embedded in their businesses. Moreover, the financial losses and economic impact were magnified by the systemic risks associated with financial counterparties, business partners, and macroeconomic and intercountry linkages. In the aftermath, governments and regulators have imposed much higher regulatory standards and capital requirements. As a result, corporate boards and executives have accelerated their investments in ERM.

An integral part of ERM is the development of key risk metrics, exposure limits, and governance and oversight processes to ensure enterprise-wide risks are within acceptable and manageable levels. A best-practice approach to addressing these requirements is to implement a clearly defined risk appetite statement (RAS). Corporate directors who are ultimately responsible for overseeing the risk management of their companies recognize this need. According to a 2013-2014 National Association of Corporate Directors (NACD) survey, only 26% of companies have a defined risk appetite statement.[2]

An RAS provides a framework for the board of directors and management to address some fundamental questions with respect to strategy, risk management, and operations, including:

- What are the strategies for the overall organization and individual business units? What are the key assumptions underlying those strategies?
- What are the significant risks and aggregate risk levels that the organization is willing to accept in order to achieve its business objectives? How do we establish governance structures and risk management policies to oversee and control these risks?
- How do we assess and quantify the key risks so that we can monitor our exposures and key trends over time? How do we establish the appropriate risk tolerances given our business objectives, profit and growth opportunities, and regulatory requirements?
- How do we integrate our risk appetite into strategic and tactical decision making in order to optimize our risk profile?
- How do we establish an ERM feedback loop and provide effective reporting to the board and senior management?

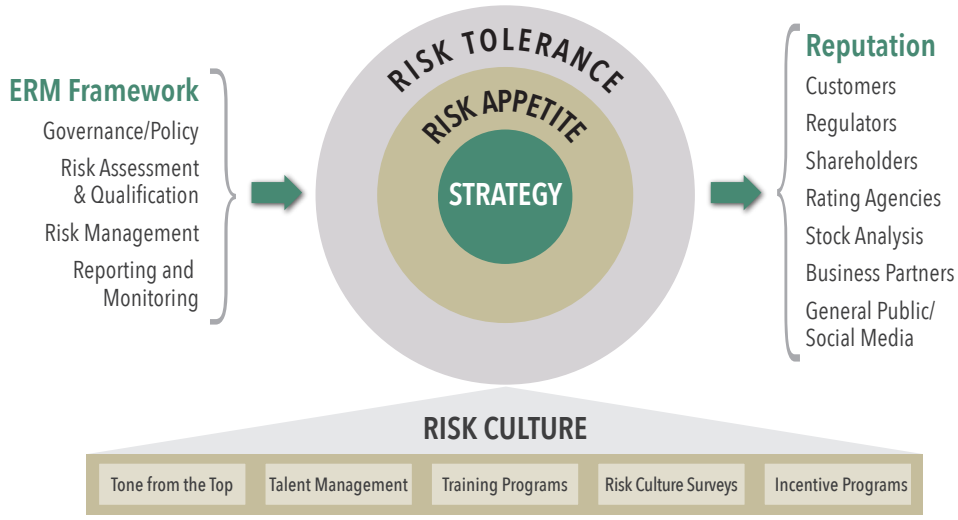
[1] James Lam, *Enterprise Risk Management: From Incentives to Controls*, Second Edition, Wiley, 2014.
[2] National Association of Corporate Directors, "Public Company Governance Survey," 2013-2014.

This Statement on Management Accounting (SMA) provides board members, corporate executives, and the risk, compliance, and audit professionals who support them with a set of guidelines, best practices, and practical examples for developing and implementing an effective RAS framework. Moreover, a maturity model is provided to help an organization assess its current state of RAS implementation, with useful benchmarks included for further development. The SMA will discuss:

- Requirements of a risk appetite framework, including key concepts and definitions.
- Developing an RAS, including implementation steps and ongoing refinement.
- Roles and responsibilities of the board, senior management, and business and operating units.
- Monitoring and reporting processes, including linkages between the RAS metrics at different levels of the organization.
- A practical example of an RAS with illustrative metrics and risk tolerance levels by key risks.
- An RAS maturity model that provides benchmarks to support self-assessment and benchmarking.

A well-developed RAS has the following attributes: (1) It is a key element of the overall ERM framework; (2) it is aligned with the business strategy and expressed with quantitative risk tolerances; (3) it reinforces the organization's desired risk culture; and (4) it produces better risk-adjusted business performance, thus enhancing the organization's reputation with its key stakeholders. Figure 1 provides an overview with these key attributes and the linkages between ERM, risk appetite, risk culture, and reputation.

FIGURE 1: THE KEY LINKAGES BETWEEN ERM, RISK APPETITE, RISK CULTURE, AND REPUTATION



Requirements of a Risk Appetite Framework

A *risk appetite statement* is a board-approved policy that defines the types and aggregate levels of risk that an organization is willing to accept in pursuit of business objectives. It includes qualitative statements and guidelines as well as quantitative metrics and exposure limits.

The RAS is implemented through a *risk appetite framework*, which includes the common language, policies, processes, systems, and tools used to establish, communicate, and monitor risk appetite. The risk appetite framework should incorporate the following elements:

- **Risk capacity** (also known as risk-bearing capacity) represents a company's overall ability to absorb potential losses. Risk capacity can be measured in terms of cash and cash equivalents to meet liquidity demands and in terms of capital and reserves to cover potential losses. Companies in highly regulated industries, such as banking, may define their risk capacity conservatively as the capital set aside to absorb potential losses under adverse scenarios. This may be the capital that would permit them, for instance, to pass regulatory stress tests. Other companies, such as technology startups, might have a more aggressive definition of risk capacity that encompasses the capital and resources that could be lost to a point just shy of insolvency in a relatively short timeframe (e.g., the next round of funding). The commonality among these calculations, however, is that they represent the absolute maximum loss a company is able (not simply willing) to take on. Risk capacity should also consider an organization's skills, tools, and performance track record in managing risks. Consider two companies with similar risk profiles and capital levels—the one with superior risk management would have higher risk capacity.
- **Risk profile** is a snapshot of an organization's risk portfolio at a specific point in time (past, present, or future). It is crucial for the risk profile to align with the business model and strategy of the organization.[3] For example, one company may choose to be a low-cost provider, in which its risk profile is driven by low profit margin (i.e., weak pricing power) and significant operational risks (e.g., cost control, supply-chain management, and scale economics). Conversely, another company could choose to be a high-quality, value-added provider, where its risk profile is driven by a high profit margin and significant strategic and reputational risks (e.g., product innovation and differentiation, customer experience, and brand management). The current risk profile of an organization is determined by all of the underlying risks embedded in its business activities, whereas the projected or target risk profile would also include business plan assumptions.

[3] At a basic level, a risk profile can be expressed in mainly qualitative terms (low, moderate, high). At a more advanced level, a risk profile will have a strong quantitative component that can be captured in a "bell curve" with a full range of probabilities and outcomes. In essence, the risk profile becomes a risk/return profile that quantifies expected performance, downside risk, and upside risk.

It is also important to understand the shape of the risk/return profile, which may have a normal or asymmetrical distribution. The risk/return profile differs by risk type and business activity. For example, credit risk in the commercial lending business has limited upside (loan margin) and significant downside (loan principal). Interest rate and foreign-exchange risks in the treasury function have more of a normal distribution because interest rates and exchange rates can equally move for or against the company. Strategic risk in the corporate research and development (R&D) budget or a venture capital fund has limited downside (value of the initial investment) but significant upside (many multiples of the initial investment). The core objective of ERM is to optimize the shape of the risk/return profile of the organization.

- **Risk-adjusted return** provides the business and economic rationale for determining how much risk an organization *should be* willing to accept. In fact, an organization should not be willing to accept any risk if it is not compensated appropriately. Conversely, if the market is providing higher expected return, then an organization should be willing to increase its *risk appetite* (while considering its *risk capacity* as discussed previously). At the inception of any business transaction, the risk originator must establish an appropriate risk-adjusted price that fully incorporates the cost of production and delivery as well as the cost of risk (i.e., expected loss, unexpected loss or the cost of economic capital, insurance and hedging costs, and administrative costs). The importance of risk-adjusted pricing cannot be overstated. Although every business takes risks, there is just one opportunity to be compensated for them—in the pricing of its products and services. In addition to pricing, organizations use a range of tools—Economic Value Added (EVA®), economic capital (EC), and risk-adjusted return on capital (RAROC)—to measure risk-adjusted profitability, evaluate investment and acquisition opportunities, and allocate capital and other corporate resources.
- **Risk appetite represents** the types and aggregate levels of risk an organization is willing to take on to actively pursue its strategic objectives. It should fall within the broader umbrella of risk capacity and, in the best possible scenario, will align closely with the organization's current risk profile. A high risk appetite will consume a greater portion of risk capacity, while a low risk appetite will consume a smaller portion, thus providing a greater buffer zone and reducing the vulnerability of the organization's capital and resources. A company's risk profile should closely resemble its risk appetite. In reality, however, it is very challenging for companies to have a clear understanding of their enterprise risk profile, which may be masked by risk assessments created in organizational silos, poorly understood risk correlations, and inadequate analysis of earnings and value drivers. Gaining a full understanding of a company's risk profile—and, subsequently, its risk appetite—is what makes an RAS particularly valuable. When a company's risk profile is out of sync with its risk appetite, management should make course corrections to bring the two closer in line.
- **Risk tolerance** is often used as a synonym for risk appetite, but in practice it is quite different and plays an important role in the risk appetite statement. Risk tolerances are the quantitative thresholds that allocate the organization's risk appetite to specific risk types, business units, product and customer segments, and other levels. Certain risk tolerances are policy limits that should not be exceeded except under extraordinary circumstances (hard limits), while other risk tolerances are guideposts or trigger points for risk reviews and mitigation (soft limits). Whereas risk appetite is a strategic determination based on long-term objectives, risk tolerance can be seen as a tactical readiness to bear a specific risk within established parameters. Enterprise-wide strategic risk appetite is thus translated into specific tactical risk tolerances that constrain risk-acceptance activities at the business level. Risk tolerances are the parameters within which a company (or business unit or function) must operate in order to achieve its risk appetite. Once established, these parameters are communicated downward through the organization to give clear guidelines to executives and managers and also to provide feedback when they are exceeded.

For this reason, risk tolerance should always be defined using metrics that are closely aligned with how business performance is measured (i.e., key risk indicators should be closely related to key performance indicators).

Establishing risk tolerance is one of the major challenges in developing an RAS framework, but it is essential to its success. There are many ways to determine risk tolerances. It is up to each organization to determine which ones work best. Figure 2 offers some approaches that an organization may take to determine risk tolerance levels. Sometimes, a blended approach is best. For example, one may initially set a risk tolerance level using statistical analysis (95% confidence level observation) and then adjust it up or down according to management judgment.

FIGURE 2: APPROACHES TO ESTABLISHING RISK TOLERANCE LEVELS

1. Board and management judgment
2. Percentage of earnings or equity capital
3. Regulatory requirements or industry benchmarks
4. Impact on the achievement of business objectives
5. Stakeholder requirements or expectations
6. Statistics-based (e.g., 95% confidence level based on historical data)
7. Model-driven (e.g., economic capital, scenario analysis, stress-testing)

While the main purpose of an RAS framework is to establish limitation on risk, it also provides other important benefits, including:

- Developing a common understanding and language for discussing risk at the board, management, and business levels.
- Promoting risk awareness and enforcing the desired risk culture throughout the organization.
- Aligning business strategy with risk management to provide a balance between financial performance and risk control requirements.
- Quantifying, monitoring, and reporting risks to ensure that they are within acceptable and manageable levels.
- Embedding risk assessments and risk/return analytics into strategic, business, and operational decisions.
- Integrating risk appetite with other ERM tools, including risk-control self-assessments (RCSAs), key performance indicators (KPIs) and key risk indicators (KRIs), economic capital, and stress-testing.
- Meeting the needs of external stakeholders (e.g., regulators, investors, rating agencies, and business partners) for risk transparency, safety and soundness, and environmental and social sustainability.

Developing a Risk Appetite Statement

The development of the RAS is an important component of an ERM program. It provides significant strategic, operational, and risk management benefits because it informs risk-based decision making for the board of directors, executive management, risk control and oversight functions (risk, compliance, and internal audit), and business and operating units. The implementation requirements for an RAS depend on the size and complexity of the organization, the business and regulatory environment in which it operates, and the maturity of its ERM program. The following provides some general guidelines for developing an RAS and for refining it on a continual basis.

Step 1: Assess Regulatory Requirements and Expectations

As part of a larger ERM effort, an RAS offers far greater value than merely meeting regulatory requirements. Nonetheless, aiding the process of meeting such requirements is a significant benefit. Whether or not it is actually required by specific laws, regulations, or industry standards, an RAS offers a systematic and holistic approach to control risk exposures and concentrations. Successful deployment of an RAS can address the requirements of several common regulatory schemes. Consider the following examples from the financial services industry:

- **U.S. Securities & Exchange Commission (SEC).** As part of a global collaborative effort of 12 supervisory agencies from 10 countries, the SEC issued a report in December 2010 that evaluated how financial institutions have progressed in developing risk appetite frameworks, including IT infrastructures and data aggregation capabilities.[4]
- **Federal Reserve (Fed).** The Fed's *Consolidated Supervision Framework for Large Financial Institutions*, released in 2012, directs that each firm's board of directors, with support from senior management, should "maintain a clearly articulated corporate strategy and institutional risk appetite." It further stipulates "that compensation arrangements and other incentives [be] consistent with the corporate culture and institutional risk appetite."[5]
- **Financial Stability Board (FSB).** In November 2013, the FSB increased the regulatory guidance on ERM and the RAS framework. This regulatory guidance included key terms and definitions and, more important, established regulatory expectations for the board.[6]
- **U.S. Office of the Comptroller of the Currency (OCC).** In 2014, the OCC set forth guidelines for financial institutions that include "a comprehensive written statement that articulates the bank's risk appetite, which serves as a basis for the risk governance framework."[7]

[4] Securities & Exchange Commission, "Observations on Developments in Risk Appetite Frameworks and IT Infrastructures," Senior Supervisors Group, December 2010.
[5] Board of Governors of the Federal Reserve, *Consolidated Supervision Frameworks for Large Financial Institutions,* 2012.
[6] Financial Stability Board, Principles for an *Effective Risk Appetite Framework*, November 12, 2013.
[7] U.S. Office of the Comptroller of the Currency, www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-4.html.

- **Own Risk and Solvency Assessment (ORSA).** Instituted by the National Association of Insurance Commissioners (NAIC) in 2014, ORSA affirms that "a formal risk appetite statement, and associated risk tolerances and limits, are foundational elements of risk management for an insurer; understanding of the risk appetite statement ensures alignment with risk strategy by the board of directors."[8]

While these regulations are focused on banks, insurance companies, and other financial institutions, organizations in other industry sectors can benefit from the standards and guidelines they provide. Moreover, all companies should understand the RAS framework expectations established by global stock exchanges, rating agencies, and other organizations such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the International Organization for Standardization (ISO).

Step 2: Communicate the Business and Risk Management Benefits of the RAS

Senior management must set the "tone at the top" and communicate the critical role that the RAS plays in the risk-management process. This communication should come from the CEO, CFO, CRO, and other senior business leaders and be directed at key internal stakeholders. Such communication may take place in town hall meetings, workshops, corporate memos, or e-mails. It should clearly articulate the support from the board and corporate leaders and provide the implementation steps, expected benefits, regulatory requirements, industry standards, and business applications of the RAS for key stakeholders. Additionally, internal stakeholders who are responsible for developing and implementing the RAS framework should receive appropriate training.

Step 3: Organize a Series of Workshops to Develop the RAS

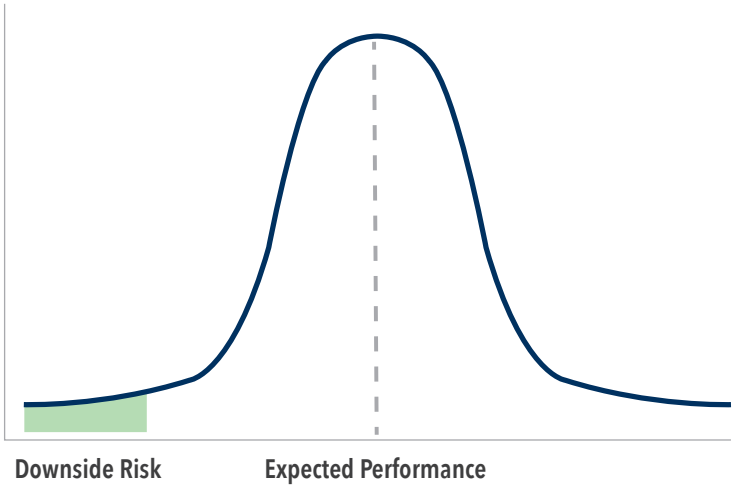
With the appropriate communication and training completed or well underway, the organization is ready to develop the RAS. The executive sponsor (e.g., the CRO or CFO) for the RAS should organize a series of workshops with risk owners (e.g., business and functional leaders) to develop the risk appetite metrics for their organizational units while the CEO and key executive team members develop the risk appetite metrics for the overall enterprise. The purpose of these workshops is to develop the RAS with input from all of the risk owners by addressing the following questions:

- **Business Strategy.** What are the business strategies and objectives for your business unit or function? What are the key assumptions underlying these strategies?
- **Performance Metrics.** What are the KPIs that best quantify the achievement of these business or process objectives? What are the performance targets or triggers for these KPIs?
- **Risk Assessment.** What are the key risks that can drive variability in actual vs. expected performance? (Note: This analysis may be provided by the risk-control self-assessment (RCSA) process.)
- **Risk Appetite.** What is our risk appetite for each of these key risks? What are the KRIs that quantify the exposure levels and/or potential loss of these risks? What are the risk limits or tolerances for these KRIs?

[8] National Association of Insurance Commissioners, *Own Risk and Solvency Assessment (ORSA) Guidance Manual,* 2014.

Figure 3 provides a diagram of the logical flow of these questions in the context of a risk/return "bell curve." Unfortunately, many companies break down this logical flow by separating the strategy and ERM components. These companies generally define strategic objectives and KPIs as part of strategic planning (Steps 1 and 2 in Figure 3) and provide reporting to the executive committee and the full board. Separately, they perform risk assessment and develop KRIs as part of ERM (Steps 3 and 4 in Figure 3) and provide reporting to the ERM committee and the risk or audit committee of the board. The integration of strategy and ERM (integrating Steps 1 through 4) provides much better analysis, insights, and decision making, including the alignment of KPIs and KRIs for the RAS framework.

FIGURE 3: DISTRIBUTION OF OUTCOMES



Integrating Strategy and ERM

1. Define business strategy and business objectives
2. Establish KPIs and performance targets based on expected performance
3. Identify risks that can drive variability in performance (risk assessments)
4. Establish KRIs and risk tolerances for critical risks
5. Provide integrated monitoring with respect to 1-4

These workshops might take place over the course of a few months. By the end of this step, the executive sponsor should be satisfied with the quality of the initial risk appetite metrics and risk tolerance levels.

The key objective of these workshops is to develop an initial set of KPIs and KRIs with their performance targets and risk tolerances, respectively. Some of the proposed metrics might be aspirational, and the risk owners will need time to develop the information. A subset of available metrics will be used to develop a prototype RAS and dashboard report in the next step.

Step 4: Develop and Socialize a Prototype RAS and Dashboard Report; Produce a Final RAS Based on Board and Business Feedback

Based on the output from Step 3, the team can produce a prototype document for the RAS to generate discussion and kick off what will become an iterative process. This document should include the RAS framework, a dashboard report with risk appetite metrics, and the RAS itself with qualitative statements and quantitative risk tolerances. (For more, see "Examples of Risk Appetite Statements and Metrics" on page 18.)

The executive sponsor can use this prototype document to socialize the prototype RAS and obtain input from corporate and business executives as well as select members of the board of directors (e.g., chairs of the risk and audit committees). Based on management and board feedback, the team can then produce a final RAS framework and dashboard report.

Step 5: Obtain Executive Management Approval

At this stage, the RAS is ready for management consideration. The executive team should take the time to thoroughly discuss and vet the RAS. This discussion may lead to changes in the risk appetite statement, metrics, and/or risk tolerance levels. Once complete, the executive committee or ERM committee would issue final approval.

Step 6: Obtain Board Approval

The RAS should next be reviewed by the board of directors, who will similarly discuss and challenge it. A key objective in this step is to establish a concise set of risk appetite metrics and risk tolerance levels that are appropriate for board-level oversight and reporting. Final approval may come from the risk committee, audit committee, or the full board.

Step 7: Communicate the RAS, including Roles and Responsibilities

After management and the board approve it, the RAS should be communicated to all employees. This is because everyone plays a role in risk management and should understand the organization's overall risk appetite and tolerances. This communication should define risk ownership as well as the roles and responsibilities for implementing the RAS framework. (See "Roles and Responsibilities" for details.)

Step 8: Review and Update Current Business Plans and Risk Policies

Ideally, the RAS would be closely aligned with the development of business plans and risk policies. The business world is dynamic and ever-changing, and the RAS must be responsive to significant changes in the competitive environment, regulatory guidance, risk-adjusted return opportunities, and the organization's risk profile and risk capacity. As such, the RAS, business plans, and risk policies should be "living documents" that are regularly reviewed and updated given key changes in the organization's business environment.

Step 9: Provide Ongoing Monitoring and Reporting

In order for the board and executive management to provide effective governance and oversight of the RAS framework, including the key risk exposures and concentrations of the organization, the ERM team must establish risk dashboard reports and monitoring processes. (See "Monitoring and Reporting" on page 15 for an example of an RAS dashboard report.)

Step 10: Provide Annual Review and Continuous Improvement

In addition to the periodic review that ensures the company's risk appetite is responsive to significant changes in the business environment, the company should conduct a formal review of the RAS at least once a year. This formal annual review includes proposed changes to the RAS framework and risk tolerance levels, alignment with business plans and risk policies, and management and board approvals.

Moreover, the organization should look for opportunities to improve the RAS framework on a continuous basis. These enhancements may include economic capital models, stress-testing and scenario analysis, technology solutions and reporting tools, broader coverage of risk, exception management plans, and integration into strategic and business decisions. (For RAS development, see "A Maturity Model" on page 22.)

Roles and Responsibilities

The process of developing, implementing, and renewing a comprehensive RAS framework should involve key stakeholders from every level of the organization. Figure 4 provides a summary of the main roles and responsibilities for the business units, executive management, and the board. The RAS itself should document specific roles and responsibilities for carrying out the risk policy, including reporting and exception-management processes.

FIGURE 4: KEY ROLES AND RESPONSIBILITIES FOR THE RISK APPETITE STATEMENT

BOARD OF DIRECTORS

Board of Directors (with Audit support)
- Review, challenge, and approve the RAS framework
- Provide risk governance and independent oversight
- Accountable for overseeing the effectiveness of the RAS, with audit support

EXECUTIVE MANAGEMENT

Executive Management (with Risk and Compliance support)
- Establish corporate strategy, RAS framework, and reporting
- Monitor aggregate risk exposures against risk tolerances
- Accountable for communicating the RAS, reinforcing the risk culture, and optimizing the enterprise risk/return profile

BUSINESS UNITS

Business Units and Functions (i.e., risk owners)
- Establish business strategies, metrics, and risk tolerances
- Report policy exceptions to executive management
- Accountable for managing the business within defined risk appetite

The "three lines of defense" model offers a lens through which to view the risk governance structure and roles defined in the RAS:

- **Business units (first line of defense)** are ultimately responsible for measuring and managing the underlying risks in their business units (i.e., profit centers) or functional units (i.e., support functions

such as HR or IT). In effect, they are the "risk owners." Business units represent the first line of defense because they are closest to risk acceptance and mitigation activities. They also have first-hand knowledge and experience in managing the risks that they face, including potential business impacts.

As active participants in the workshop meetings discussed previously in Step 3, the business and functional leaders are also responsible for defining their business strategies and aligning them with the appropriate risk appetite and risk tolerances. Once the RAS is established, they must report policy exceptions to the CRO and/or executive management. The business and functional units are ultimately accountable for how well their businesses and operations perform vis-à-vis the risk tolerances established in the RAS.

- **Executive management with the support of risk and compliance functions (second line of defense)** is responsible for developing and communicating the RAS framework. The CRO (or equivalent) should lead this effort. The CEO, with the support of the executive management team, establishes the overall corporate strategy and ensures that business-unit strategies are aligned. Executive management is also responsible for defining the risk appetite and risk tolerances at the enterprise level and providing ongoing reporting to the board and other key stakeholders (e.g., rating agencies, institutional investors).

  The CRO and the ERM team are responsible for developing tools to measure and monitor aggregate risk exposures against risk tolerances. They also must provide business context, expert analyses, and root causes for any risk tolerance breaches. Executive management is ultimately held accountable for how well it optimizes the risk/return profile of the organization and for the strength of its risk culture.
- **The board with the support of internal audit (the third line of defense)** is responsible for reviewing, challenging, and approving the RAS framework. Once the RAS framework is in place, the role of the board shifts to providing independent oversight. The risk or audit committee may take the lead in this ongoing process. It is also the responsibility of the risk or audit committee to step in when it sees exposures that are consistently above risk tolerances or if a business or functional unit does not demonstrate a strong risk culture. These failures may require a "deep dive" to investigate and rectify them. On the other hand, if risk limits and tolerances are never exceeded (i.e., no policy exceptions over an extended period of time), then the board may reasonably question whether the RAS tolerances are too high or lax to be effective.

  The board is ultimately responsible for ensuring that an effective ERM program is in place, including a robust RAS framework. To fulfill this critical fiduciary responsibility, the board requires timely, concise, and effective risk reporting from management, usually in the form of an RAS dashboard. This dashboard should clearly highlight any risk metric that falls outside its associated tolerance (e.g., by showing it in a "red zone") and include commentary that explains the root causes for the policy exception along with management's plans and timeframe for remediation.

Monitoring and Reporting

The venue and timeframe for RAS monitoring will vary based on the business, function, and organizational level. For example, IT may monitor tactical risk metrics and warnings on a real-time basis in its datacenter "war room" where IT performance and risk indicators are displayed across multiple interactive screens. A business unit, and the ERM function, may monitor key business and risk metrics on a weekly basis, with more formal monthly or quarterly reviews. Executive management and the board would monitor the RAS based on their committee schedules.

An effective RAS dashboard reporting process should be structured to produce consistent reports at various levels of the organization. The number and types of metrics would likely vary with the target audience. Figure 5 provides an illustrative example of an RAS dashboard reporting structure. The report is organized into five primary risk categories: strategic/business, financial, operational, compliance, and reputational. Each risk category has metrics that are assigned a risk tolerance or range that acts as limits or guidelines for acceptable risk exposures. These metrics are tracked over the previous four quarters.

FIGURE 5: RISK APPETITE DASHBOARD STRUCTURE

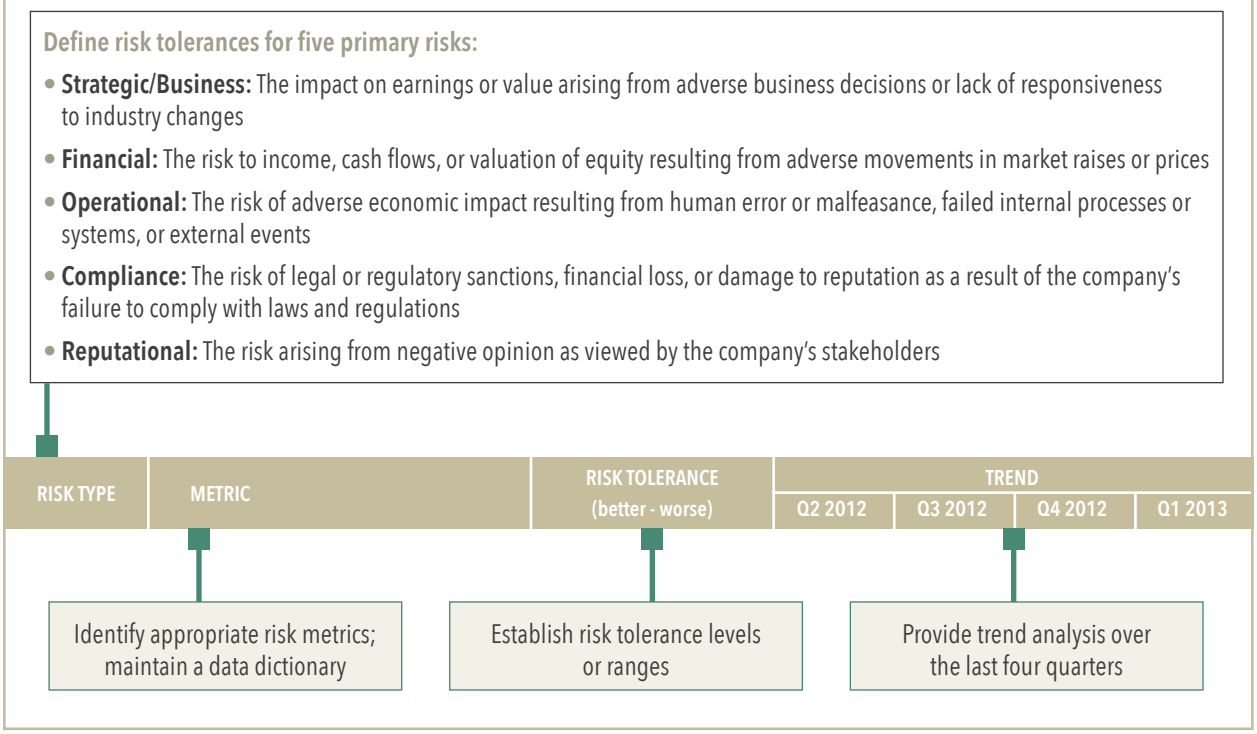


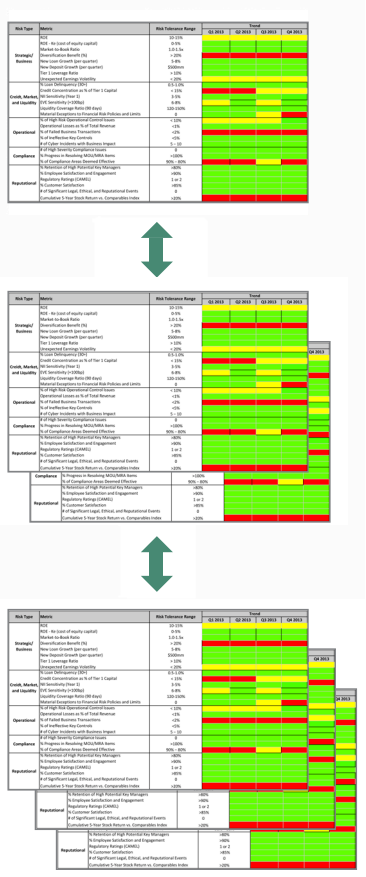
Figure 6 shows an illustrative RAS dashboard report with specific metrics and tolerance levels for each major risk type. It is important to note that the RAS is meant to capture only the most critical risks. Otherwise, it would be far too unwieldy to be effective. By pinpointing the most useful risk metrics, the RAS aims to provide an overall, holistic view of the company's risk profile. For instance, it should identify KRIs that are linked to the main drivers of short- and long-term performance in order to warn of potential unacceptable business outcomes and trigger corrective actions.

FIGURE 5: RISK APPETITE DASHBOARD STRUCTURE

RISK TYPE	METRIC	RISK TOLERANCE RANGE	TREND			
			Q2 2012	Q3 2012	Q4 2012	Q1 2013
STRATEGIC/ BUSINESS	ROE	10%–15%				
	ROE – Ke (cost of equity capital)	0%–5%				
	Market-to-Book Ratio	1.0x–1.5x				
	Diversification Benefit (%)	>20%				
	New Loan Growth (per quarter)	5%–8%				
	New Deposit Growth (per quarter)	$500mm				
	Tier 1 Leverage Ratio	>10%				
	Unexpected Earnings Volatility	<20%				
CREDIT, MARKET, AND LIQUIDITY	% Loan Delinquency (30+)	0.5%–1.0%				
	Credit Concentration as % of Tier 1 Capital	<15%				
	NII Sensitivity (Year 1)	3%–5%				
	EVE Sensitivity (+100bp)	6%–8%				
	Liquidity Coverage Ratio (90 days)	120%–150%				
	Material Exceptions to Financial Risk Policies and Limits	0				
OPERATIONAL	% of High-Risk Operational Control Issues	<10%				
	Operational Losses as % of Total Revenue	<1%				
	% of Failed Business Transactions	<2%				
	% of Ineffective Key Controls	<5%				
	# of Cyber Incidents with Business Impact	5-10				
COMPLIANCE	# of High Severity Compliance Issues	0				
	% Progress in Resolving MOU/MRA Items	>100%				
	% of Compliance Areas Deemed Effective	90%-80%				
REPUTATIONAL	% Retention of High-Potential Key Managers	>80%				
	% Employee Satisfaction and Engagement	>90%				
	Regulatory Ratings (CAMEL)	1 or 2				
	% Customer Satisfaction	>85%				
	# of Significant Legal, Ethical, and Reputational Events	0				
	Cumulative Five-Year Stock Return vs. Comparable Index	>20%				

An effective RAS should provide a "cascading" structure of risk exposures and limits at the board, executive-management, and business-unit levels. This structure allows for drilling down to underlying exposures (e.g., "What business activities make up our strategic risk exposure to China?"). Similarly, this structure permits aggregation of business-level exposures upward to the enterprise level (e.g., "What is our total net credit exposure to Goldman across the entire enterprise?"). The level of detail visible for each metric depends on the needs of the specific audience (i.e., board, corporate management, or business unit). Figure 7 provides an illustration of cascading risk appetite statements at the three levels of the organization. As shown, the RAS would be at its most dynamic at the business level, where managers may choose to make changes based on risk/return opportunities while respecting board- and management-level risk tolerances.

FIGURE 7: CASCADING AND DYNAMIC RISK APPETITE STATEMENTS



Level 1: Board

- Focus on strategic and other significant risks
- 30-35 metrics
- Changes are rare and exceptional

Level 2: Executive Management

- Focus on business and operational risks
- 60-80 metrics
- Changes are infrequent

Level 3: Business Segments

- Focus on business and operational risks
- Number of metrics depends on business-specific requirements
- Changes driven by risk/return opportunities

Certain types of risk metrics can readily be aggregated across the organization, while others are unique to specific business and operational units. Since the board and executive management RAS reports are focused on strategic and enterprise-wide risks, the risk metrics that can be aggregated should be well represented in these reports. Such metrics include:

- Earnings-based, including earnings-at-risk and unexpected earnings volatility.
- Value-based, including shareholder value-added and market/book ratios.
- Loss-based, such as actual losses, operational loss-to-revenue ratios, stress-testing, or scenario-based losses.
- Cash-flow-based, such as cash-flow-at-risk and liquidity-coverage ratios.
- Financial risk metrics, including market risk and credit/counterparty risk exposures.
- Number of incidents, such as policy exceptions, cyberattacks with business impact, and legal and regulatory issues.
- Key stakeholder metrics, such as retention of high-performance employees or levels of customer satisfaction.

Finally, the RAS should provide a "common language" for the ERM program. This would consist of a glossary of relevant business or technical terms and acronyms as well as a data dictionary that describes each risk metric, how it is calculated, where the underlying data is generated, and why it is included.

Examples of Risk Appetite Statements and Metrics

The following sections provide examples of risk appetite statements, performance and risk metrics, and risk tolerance levels for the following risk categories: enterprise-wide risk, strategic risk, financial risk, operational risk, legal/compliance risk, and reputational risk. For simplicity, each risk appetite statement is paired with one or two example metric(s) and risk tolerance level(s). In practice, there may be a number of risk metrics and risk tolerances for each risk appetite statement.

Enterprise-wide Risk Management

The objective of our ERM program is to minimize unexpected earnings volatility and maximize shareholder value. The following risk appetite statements, metrics, and risk tolerances are in support of this overarching objective:

- **Business Objectives.** Our ERM program is integrated into our business decision making, and our risk mitigation and management strategies are designed to enhance the likelihood of achieving our business objectives.

  Metric: Any shortfall between actual vs. expected performance of our top strategic objectives will be less than 10%.

- **Investment-Grade Debt Rating.** Our capital adequacy and debt coverage will be maintained to achieve an investment-grade rating from all of the major rating agencies. Moreover, we will maintain surplus capital and liquidity reserves to support future growth and buffer against economic uncertainties.

  Metric: Debt ratings from the major rating agencies will be at least investment grade; Surplus capital and liquidity will exceed 15% of total requirements.

- **Unexpected Earnings Volatility**. We will perform earnings-at-risk (ex-ante) and earnings attribution (ex-post) analyses and target unexpected earnings variance to be a reasonable portion of total earnings variance.

  Metric: Monthly unexpected earnings volatility (i.e., earnings variances from unexpected sources) will be less than 20% of total earnings variance.

- **ERM Maturity.** We will continue to develop our ERM capabilities to ensure that a best-in-class ERM program is in place. Based on the size and complexity of our business, we will achieve an "excellent ERM" assessment from independent third parties within three years.

  Metric: Completion of the three-year ERM roadmap initiatives and milestones will be at least 90% in the monthly tracking report.

- **Risk Culture.** All employees are expected to understand the risk associated with the business activities in which they are engaged. Every employee is accountable to operate within risk appetite standards and tolerances.

  Metric: Annual risk culture surveys will exceed defined target levels.

Strategic Risk Management

We strive to diversify our business portfolio to mitigate exposures to macroeconomic changes. Our business units will only pursue investment opportunities and business transactions that are consistent with the overall corporate strategy and our defined core competencies. We will focus our marketing efforts and technology initiatives to significantly enhance customer experience.

- **Corporate Diversification.** Our growth strategies (organic growth and M&A) will be formulated to achieve both economic value creation and diversification benefit.

  Metric: Diversification benefit will exceed 30%.[9]

- **Strategic Alignment and Core Competence Focus.** We will focus on business investments that are consistent with our overall strategy and core competencies.

  Metric: Investment capital to support noncore businesses will be less than 10%.

[9] One measurement of diversification benefit is the net reduction of economic capital requirements when correlation effects across business units are factored in. In other words, the economic capital requirement for the overall corporation is less than the sum of its parts.

- **Customer Experience.** We strive to offer a superior customer experience both online and in service centers.

  Metric: Customer satisfaction will exceed 80% in both channels.

- **Risk-Adjusted Profitability.** We will achieve an overall risk-adjusted return on capital (RAROC) that exceeds our cost of equity capital (Ke), resulting in a positive economic profit for the aggregate business and our shareholders.

  Metric: Enterprise RAROC will exceed Ke by at least 2%.

Financial Risk Management

We take financial risks in order to support our core business activities. We do not have a view of the direction of financial markets and, therefore, do not speculate on markets to generate income. We manage our liquidity position in a conservative manner for both expected and stressed business conditions.

- **Interest Rate Risk.** Our treasury department aims to manage interest rate risk within board-approved limits.

  Metric: Maximum impact on income given a 100bp parallel shift in rates is 7%.

- **Credit Risk.** Our lending activities are based on strong underwriting standards and "know your customer" principles.

  Metric: Net credit losses will be less than 1% of average loan balances.

- **Liquidity Risk.** We manage our liquidity position to ensure that we can meet our cash obligations even under liquidity stress tests.

  Metric: Maintain a liquidity coverage ratio of at least 200% under the likely scenario and at least 110% under the stressed scenario.

- **Hedging Effectiveness.** We use derivatives for hedging purposes and never to speculate. We use only permitted derivative products, and each hedge transaction must decrease the earnings sensitivity of the overall risk position.

  Metric: Hedge effectiveness ratio will exceed 80%.

Operational Risk Management

We establish and test internal control systems to prevent, detect, and mitigate operational risk exposures. Each business unit is required to identify and assess its operational risks and ensure that they are measured and managed effectively.

- **Operational Losses.** We measure and track operational losses and incidents across the organization to identify root causes, mitigate risks, and ensure that losses are within acceptable levels.

  Metric: Operational loss/revenue ratios should be less than 1% for all business units.

- **Talent Management.** We strive to establish and maintain a talented workforce, especially through the professional development and retention of high-potential employees.

  Metric: Retention rate of high-potential employees will be at least 90%.

- **Third-Party Vendor Management.** We rely on business partners and third-party vendors to provide critical services. We seek to minimize high-risk third-party vendor relationships.

  Metric: High-risk third-party vendor relationships must be exited within one year, or a viable, fully tested contingency plan must be in place.

- **IT Risk.** We manage our IT infrastructure to ensure system availability and capacity to meet business requirements as well as to protect against natural and manmade threats, including cyberattacks.

  Metric: Number of IT events with material business impact will not exceed two per month. Recovery time for critical-system failures will be within one hour.

Legal/Compliance Risk Management

We will conduct our business within the confines of all laws and regulations. Every employee is held accountable for maintaining the highest ethical standards.

- **Ethics Policy.** We have zero tolerance for violations of our corporate ethics policy.

  Metric: All exceptions to our corporate ethics policy will be reprimanded based on the severity of the violation, including termination, bonus clawback, and legal actions.

- **Open Regulatory Findings.** The number of open regulatory findings will be maintained within an acceptable level.

  Metric: Active regulatory findings will be fewer than 15.

- **New Legal Matters Opened.** The number of new legal matters opened will be maintained within an acceptable level.

  Metric: New legal matters opened each month will be fewer than five.

- **Legal and Compliance Cost.** We will control the direct cost for resolving legal and compliance issues, including fines, settlements, penalties, and outside legal and regulatory advisory expenses.

  Metric: Total legal and compliance cost each month will be less than $10 million.

Reputational Risk Management

Our reputation is extremely valuable, and it is every employee's responsibility to safeguard and indeed enhance the reputation of the company. The board, CEO, and senior management will ensure that the level of reputational risk the company assumes is managed effectively.

- **Customer Perspective.** We will enhance our customers' experience when doing business with us and address any issues in a timely and effective manner.

  Metric: Acknowledge customer complaints within 24 hours, and resolve legitimate complaints within five business days.

- **Employee Perspective.** We will strive to be the employer of choice in our industry and maintain a high level of employee satisfaction.

  Metric: Annual survey of employee satisfaction will be greater than 90%.

- **Shareholder Perspective.** We will deliver superior shareholder returns and create significant shareholder value by allocating capital to the highest risk-adjusted return opportunities.

  Metric: Stock performance will be in the top quintile against our peer group.

- **General Public and Media Coverage.** We will closely follow coverage of our company in the press, social media, and other public forums to monitor reputational risk levels.

  Metric: We have zero tolerance for headline risk associated with unacceptable business practices, privacy breaches, and internal fraud.

A Maturity Model

It generally takes months for a company to design, prototype, develop, revise, and finalize its first RAS framework. In the financial services industry, where the application of risk appetite statements has been formalized over the past several years, leading companies are implementing their second or third "generation" of their risk appetite framework.[10]

As the RAS framework is being developed and implemented, it is helpful to review the key benchmarks by way of an RAS maturity model. The purpose of the maturity model is to provide specific benchmarks of RAS practices so that companies can self-assess the maturity and development opportunities of their RAS frameworks.

The following RAS maturity model organizes the key steps of implementing an RAS framework into four stages:

[10] An Oliver Wyman/Risk Management Association survey of 65 financial institutions indicated that two-thirds reported being on their second or third "generation" of their risk appetite framework (www.rmahq.org, January 2014).

Stage 1: Qualitative RAS, Early Development

In Stage 1, the organization defines the scope of and objectives for its RAS framework. Key objectives during this phase include identifying the organization's RAS requirements, obtaining board-level and executive support, and developing an overall framework and plan for implementing the RAS. Stage 1 may take two to three months to complete. Typical activities include:

- Researching regulatory requirements and industry practices,
- Providing training for key internal stakeholders,
- Appointing an executive sponsor and establishing a project management team,
- Conducting benchmarking exercises with other companies,
- Aligning with the ERM framework and RCSA processes, and
- Developing an initial RAS with mainly qualitative risk appetite guidelines (low, moderate, high), except for quantitative financial risk metrics and risk tolerances that are more readily available.

Stage 2: Quantitative RAS, Early/Intermediate Development

In Stage 2, the organization completes most or all of the 10 steps outlined previously in "Developing a Risk Appetite Statement" on page 9. It fully develops risk appetite statements, metrics, and risk tolerances for the board, executive-management, and business-unit levels. Stage 2 may take six to nine months. Typical activities include:

- Conducting the RAS workshops;
- Developing a database and reporting process for KPIs and KRIs, with their respective performance targets and risk tolerances;
- Developing the overall RAS framework;
- Producing the RAS dashboard reports for the board and executive management on a monthly basis, including commentaries and expert analysis;
- Rationalizing the set of risk appetite metrics based on board and management feedback; and
- Integrating the business objectives, KPIs, risk assessments, and KRIs.

Stage 3: Cascading RAS, Intermediate Development

In Stage 3, the organization develops the RAS framework further to make it more actionable and valuable to the business. A key objective is to leverage the RAS to inform tactical business and operational decisions. This stage may take nine to 12 months. Activities may include:

- Developing a cascading, drill-down capability from Level 1 (board) to Level 2 (executive management) to Level 3 (business unit) risk appetite statements;
- Providing broader coverage of risk, including strategic risk and reputational risk;
- Formalizing risk-mitigation and exception-management plans;
- Establishing alignment with tactical business and operational decisions; and
- Implementing automated, collaborative reporting technologies.

Stage 4: Dynamic RAS, Advanced Development

In Stage 4, the focus is on integrating the RAS into strategic and business-management decisions. Thus, RAS metrics and reports are distributed more widely through the organization. It is during this stage that risk/return tradeoffs in business decisions are evaluated more explicitly. Stage 4 is ongoing and includes the following activities:

- Providing dynamic adjustments to business-unit RAS to reflect risk-return opportunities;
- Aligning the RAS with strategic management decisions (strategy development and execution, capital and resource allocation);
- Integrating stress-testing and scenario analyses into the RAS framework;
- Developing feedback loops on the efficacy of RAS metrics; and
- Linking risk management performance and executive compensation.

Summary

The RAS establishes a board-approved policy that aligns the organization's risk tolerances with strategic objectives, risk profile, and risk management capabilities. It is a foundational component of an effective ERM program. For the board, executive management, and business and operational staff, the RAS addresses a central question: "How much risk are we willing to accept to pursue our business objectives?"

This began with the key components of a risk appetite framework, including basic concepts and definitions. It then discussed the implementation steps and defined the roles and responsibilities for the board, senior management, and business and operating units. Linkages between the RAS metrics at different levels of the organization were examined to support enterprise-wide risk monitoring and reporting. A practical example was provided to illustrate the risk appetite statements and risk tolerances for the major risk categories. Finally, an RAS maturity model was presented to help facilitate self-assessment and continuous improvement.

The only thing certain in business is uncertainty. The RAS is an essential tool for any organization that strives to pursue its business strategy while managing all of its significant risks. By establishing strategic priorities and risk boundaries for all employees, a robust RAS that is communicated effectively can also have a profound impact on an organization's risk culture.

Acknowledgments

I would like to thank Michelle Jonson, chief risk officer at the Federal Home Loan Bank of Chicago, and Lita Cuen, enterprise risk manager at Continental Resources, for their reviews and suggestions. I would also like to thank Mark Ganem and Simone Liano of the Workiva ERM Research Team for their research and editorial support.