BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

"Why should you spend time worrying about risk appetite? Many think that it is something that board members, chief executives, and senior management intuitively know, or work out while making decisions. They may even think they don't need another document on the topic. We disagree. We need to make risk appetite an integral part of decision-making."

-Dr. Larry Rittenberg and Frank J. Martens, CPA; Risk Appetite – Critical to Success (COSO, 2020) [1]

February 28, 2023

Is Your Risk Appetite Statement More than an Academic Exercise?

By Suzanne Hartin

Risk appetite statements, which at a high level define the types and amounts of risk an organization is willing to accept in pursuit of value [2], are designed to guide organizations in their risk-taking decisions. Too often, they do not. Companies may not make effective use of risk appetite statements for many reasons – for example, the culture of risk management may not be strong, the risk appetite statement may be too vague and hard to apply, or the risk appetite statement may be too "top down" without a reality check at the business operations level. It's relatively easy to apply risk appetite parameters in environments where a business is singularly focused and good metrics abound. But what if the risks related to products and services are a little harder to measure? What if you are a health care or entertainment company? What then?

More Helpful Versus Less Helpful Risk Appetite Statements

A useful risk appetite statement needs to be developed within a risk appetite framework (RAF), the key elements of which help frame and define the company's risk appetite. The risk appetite framework is the overall approach and structure, including policies, processes, controls, and systems through which risk appetite is established, communicated, and monitored. It includes a risk appetite statement, risk limits, as well as documentation of the roles and responsibilities of those overseeing the implementation and monitoring of the framework. The RAF should consider material risks to the organization, as well as to the company's reputation with investors and customers. The RAF must align with the institution's strategy [3].

A risk appetite statement is derived based upon how much risk and of what type, the company is willing to take in the pursuit of its goals. Is a company willing to take a significant amount of strategic or reputational risk when moving into new business lines? Is the company less willing to take compliance or legal risk? How much? In order for risk appetite statements to actually be useful in guiding business decisions, businesses should understand specific risk tolerances, and the extent to which those tolerances can be exceeded for short periods in specific circumstances.

A few years ago, I attended a discussion at a risk management conference centered around risk appetite statements and risk tolerance. Part of the discussion focused on whether internal expressions of risk appetites and tolerance could be shared publicly. In most cases they could be, even though they usually are not. A cruise line gave an example where their internal risk tolerance was not something they would ever state publicly: externally, their risk messaging declared that the company's tolerance for passengers overboard was zero, but internally, the company's official limit was one passenger overboard per year. The reason for this discrepancy was that the cruise line could never invest enough money in training, guard rails, and other safety measures to guarantee that no one would ever go overboard. But the company felt it could never say that passenger overboard situations were, in fact, a rare but real occurrence.

In my own experience, I've seen the same thing. Having a zero tolerance for security incidents is the quickest way to put a company out of business. Today most firms can't be in business and have no cyber security risk. But it would be extremely problematic to publicly share that you have some tolerance for security incidents.

The most helpful risk appetite statements are simple, specific and measurable, such as "We will implement programs and controls such that fraud is contained to less than X basis points per month" or "We will control credit losses to no more than X basis points per quarter." While an organization may not be able to craft this sort of simple statement for the entire business, the company may be able to do so for many parts of the business.

For businesses where the risks are less straightforward to measure, a more general risk appetite statement can still be useful. Consider this one:

> Generally, the Company's highest priority and lowest risk appetite relates to information security, protecting customer data and compliance with regulatory standards. We will take risks in a well controlled manner to maintain our competitive position, strengthen our reputation and innovate to achieve our strategic objectives. In the event of competing priorities, the Executive Committee shall review and propose an appropriate approach and related implementation timeframes consistent with our highest priority and risk appetite statements.

To put a statement such as this into practice organizations would need to develop business-line specific definitions of the various types of risk they would expect, along with metrics and thresholds that represent acceptable levels of risk taking for each category of risk.

There is generally a continuum of risk measures for each risk type that indicates "within appetite and acceptable," "somewhat outside of appetite (above or below) but temporarily acceptable with a plan to mitigate a risk and return to appetite limits" and "outside of appetite and unacceptable." With the statement defined and risk performance measures in place, the company can then evaluate various tradeoffs to ensure the risk types with the lowest risk appetite are well controlled while allowing more leeway for taking other types of risk.

Questions the Board should ask:

1. How did Management develop the risk appetite statement? Was the process comprehensive (input from and socialized at all levels)?
2. Are emerging risks that could be material to the company considered?
3. Is the risk appetite statement inclusive? Could it be used to evaluate forward looking initiatives (e.g., potential acquisitions or divestments)?
4. Do we agree with the risk appetite statement?

Putting the Risk Appetite Statement to Work

Significant business decisions are rarely one-dimensional. Business propositions should consider multiple types of risk, including financial, reputational and strategic risk as well as risks such as legal, compliance, regulatory and so on. For instance, if a pending decision has to do with offering a new product, there might be strategic, market, reputational, security, technology, compliance, and other risk considerations. The key is how these various factors are considered against one another. For instance, a company might be willing to take more strategic and reputational risk up front as the strategy or new product is being envisioned and designed at a high level. However, there might be a more conservative approach with less risk-taking during final design and implementation to ensure that all compliance, legal, and customer experience requirements are met.

So, how should management and the board ensure that the risk appetite statement and associated risk tolerances are considered at every step of the decision-making process? The key is embedding risk appetite into the various parts of the business decision process, ensuring risk partners are at the table wherever appropriate.

- First, when a new strategy is being considered, incorporate structured discussions about the level and types of risk implementing that strategy would bring to the company. Would it raise the public profile of the company and invite more regulatory or legal scrutiny or entice more bad actors to target the company from a cyber perspective? Would it vault the company ahead of its competitors, reducing market or strategic risk? Is it such a big bet that it would materially impact the company's financials?
- Second, as projects or products are defined at the high-level to support the strategy, require that risk considerations are documented in business cases and funding requests.
- Third, as project plans are refined, require that more detailed considerations of risk are included in the artifacts of the project and that they are discussed at defined control points in the project development lifecycle. This will make it much easier for the company's risk professionals to evaluate whether the risk appetite statement is being adhered to, enables them to perform product or other risk assessments, and allows active support for the company's activities in fulfilling its vision.
- Fourth, whenever management conducts internal business reviews, include a discussion of risk considerations: how the risks were evaluated and what is being done to address them. This transparency allows for robust risk conversations and ensures that project goals can be achieved with a minimum of risk related diversions.

Questions the Board should ask:

1. Where and how is the risk appetite statement leveraged for decision making?
2. Do we see evidence of this use?
3. Is this sufficient (when used, where used and outcomes)?

Creating, Updating and Reporting on the Risk Appetite Statement

The initial creation and subsequent updating of a risk appetite statement should result from a collaboration at different levels across entities, large and small. Often the driving force in the creation and cyclical refresh of risk appetite statements may be the risk, compliance or legal organizations. No matter where the responsibility lies, the effort must be led by individuals with the capacity and internal stature to lead a collaborative process across the organization. Typically, a draft risk appetite statement will be created and circulated for input by executives, business line leaders, risk professionals and others. It's critical that those who will be applying the risk appetite statement and measuring risk performance against it are allowed sufficient time and opportunity to appropriately influence the statement's design.

Once a final draft is complete, it is reviewed at appropriate organization check points for approval. These check points will vary by organization type and size but should end with board review and approval.

Risk appetite statements should be reviewed regularly since the risk environment, a company's business activities and other influencing factors can change quickly. At a minimum, the statement should be reviewed and updated annually, and require board sign-off. Any material risk, product or other changes between the annual cycle should be reviewed and approved by the Board.

On a regular – quarterly or semi-annual – basis boards should review a set of metrics that display risk performance against risk appetite (see example). The dashboard should cover the complete suite of material tracked risks, and should highlight sets of risks that may still be below threshold but are trending in the wrong direction. There should be an agreement with the Board on specific thresholds at which any out-of-appetite metrics would be reviewed with the Board for a discussion about how management is addressing the risks and on what timeline.

Questions the Board should ask:

1. What information informs changes to the risk appetite statement?
2. Is the refresh process frequent enough?
3. Does reporting against the risk appetite statement give a comprehensive view of whether risk performance is within appetite or not?
4. Do we agree with management on the escalation thresholds for risk performance outside of appetite?

TO BE EFFECTIVE, APPETITE MUST BE:

- Operationalized through appropriate tolerances, and where necessary, codified through policy
- Stated in a way that assists management in decision making
- Precise enough to be useful in making decisions and in monitoring by management and others responsible for managing risk
- Applied by those with decision-making authority from the board through senior and middle management on down into the entity

- From Risk Appetite – Critical to Success (COSO, 2020)
COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf

REFERENCES

[1] Dr. Larry Rittenberg, Ernst & Young Emeritus Professor of Accounting at the University of Wisconsin Madison School of Business, Frank J. Martens, CPA, Pacific Rim Risk Management Services Ltd; *Risk Appetite – Critical to Success (COSO, 2020)*, **COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf**

[2] COSO ERM 2017 page 110

[3] Financial Stability Board, 2013

ABOUT THE AUTHOR

Suzanne Hartin
Chief Risk Officer, Early Warning Services

As chief risk officer for Early Warning Services, the network operator of Zelle, Suzanne Hartin leads the company's risk functions including Information Security, Enterprise and Operational Risk Management, Business Continuity and Crisis Management, Third Party Risk Management, Compliance, Privacy, and Physical Security.

Ms. Hartin has over 20 years of risk management experience developed at a variety of the nation's largest financial institutions. Prior to joining Early Warning, she was Vice President of Operational Risk Management at Capital One where she managed the Enterprise Business Continuity and Crisis Management teams as well as the Corporate Third Party Risk Management and Corporate Insurance Risk Management programs. She has also held a number of executive risk, compliance and information security positions at American Express and Bank of America. While performing in these roles, she obtained extensive experience being examined by the OCC, the CFPB and other regulatory agencies.

Ms. Hartin graduated from Davidson College with a degree in economics and is a Certified Information Security Manager (CISM) and is Certified in Risk and Information Systems Controls (CRISC). She serves on the Board of Directors for Sytek Electric, the world leader in design and manufacture of high-powered sub-sea motors used on ROVs (remotely operated vehicles) and other sub-sea applications, and is a member of the Executive Women's Forum (EWF).

UPCOMING EVENT

16th Annual Shared Assessments Third Party Risk Summit
March 15-16, 2023
Orlando World Center Marriott, Orlando, FL

The Shared Assessments Third Party Risk Summit is the premier global, multi-industry event to shed light on processes, technologies and efficiencies in third party risk management. Join leading experts in risk management to identify trends, leverage new technologies, and share best practices.

****The BRC will lead a breakout session on Day Two of the Summit titled, "Board Risk Communications: How Much is Enough? Best Practices for Presenting Risk to Board Directors."***

The Board Risk Report *is the periodic publication of the BRC.* ***SUBSCRIBE NOW*** *to receive complimentary world-class risk management practices delivered directly to your inbox.*

WHO WE ARE

The Board Risk Committee (BRC) is the foremost thought leadership peer council for board risk committee members and chief risk officers. The BRC is a nonprofit, non-competitive, trusted place for the exchange of ideas, strategies, and best practices in enterprise risk oversight. We advocate for having risk committees of boards, where appropriate, and for educating board directors about enterprise risk. The BRC aims to foster more effective risk management and board oversight. The BRC works in partnership with The Santa Fe Group (SFG) and Shared Assessments (SA). SFG is a strategic advisory company providing expertise to leading corporations and other critical infrastructure organizations in the area of risk management. SA is the thought leader and provider of tools, education and certifications in the third party risk management space. *The Board Risk Report is the periodic publication of the BRC.*

BRC Contacts:
Catherine A. Allen, Founder and Chair of the Board, cathy@boardriskcommittee.org
Ellen Dube, Executive Director, ellen@boardriskcommittee.org
Susan C. Keating, Chief Partnership Officer, susan@boardriskcommittee.org