Brought to you by:

PROTECHT

Risk Appetite

for dummies

A Wiley Brand

Create an effective risk appetite statement

Define risk appetite to support your objectives

Embed risk appetite in your business

Protecht Special Edition

David Tattam

Brett McLaughlin

About Protecht

While others fear risk, we embrace it. For over 20 years, Protecht has redefined the way people think about risk management. We help companies increase performance and achieve strategic objectives through better understanding, monitoring, and management of risk.

We provide a complete solution comprised of world-class risk management, compliance, training, advisory, and consulting services to businesses, regulators, and governments across the world.

With our flagship Protecht ERM SaaS platform, you can dynamically manage all your risks in a single place: risks, compliance, incidents, KRIs, vendor risk, IT and cyber risk, internal audit, operational resilience, business continuity management, occupational safety and health, and more.

We're with you for your full risk journey. Let's transform the way you understand and manage your risk to create exciting opportunities for growth.

Find out more about Protecht at protechtgroup.com.

Risk Appetite

Protecht Special Edition

by David Tattam and Brett McLaughlin

for dummies®
A Wiley Brand

Risk Appetite For Dummies®, Protecht Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-23785-2 (pbk); ISBN 978-1-394-23786-9 (ebk); ISBN 978-1-394-28306-4 (epub)

Printed in Singapore and the United States

Publisher's Acknowledgments

Project Editor: Kerry Laundon

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Business Development Representative: Molly Daugherty

Content Refinement Specialist: Saikarthick Kumarasamy

Protecht Special Help: John Band, Project Manager; Michael Howell, Specialist Adviser; Karen Haas, Content Reviewer; Megan Connell, Project Director

Table of Contents

Introduction

Risk appetite is how much risk an organization is willing to accept, retain or take in pursuit of its objectives. It should be used as a core part of any risk management framework, including to evaluate whether the right amount of risk is being taken, to support assurance and early warnings through risk appetite-based reporting, and to aid risk-versus-reward decision-making. It should also guide behavior by influencing culture.

Every organization has a risk appetite — but for many, it is implied rather than actively determined. As a result, developing an explicit top-down risk appetite is an essential component of a true enterprise approach to risk management.

Since risk is the effect of uncertainty on objectives, an organization's risk appetite is the amount of uncertainty it is willing to accept in relation to achieving its objectives. Setting the right level of risk appetite is crucial. Setting a lower risk appetite will ensure fewer things go wrong but could hold your organization back from pursuing opportunities and achieving success. Setting a higher risk appetite can open more avenues of opportunity but may lead to negative events that could result in lasting damage to your organization.

While the risk appetite statement should be owned by the board, a well-defined and embedded risk appetite is critical for business executives, risk professionals, and stakeholders alike. Embedding risk appetite in your business enables executives and staff at all levels to make better decisions and ultimately take better advantage of business opportunities.

About This Book

This book is a guided tour to understand, define, and apply risk appetite. In Chapter 1, you'll be introduced to the concept of risk appetite and its significance. Chapter 2 digs deeper, addressing modern methods to articulate risk appetite in alignment with business goals. Chapter 3 guides you through the practicalities of how to craft a risk appetite statement (RAS), the critical tool you'll use to express your organization's risk boundaries at the highest level.

Chapter 4 equips you with strategies to embed risk appetite within your business. Chapter 5 rounds out the exploration with ten actionable tips to inform you as you develop and apply risk appetite. By the end of the book, you'll have a comprehensive understanding of risk appetite's role in today's ever-evolving risk and overall business landscape.

Icons Used in This Book

Throughout this book, you'll encounter specific and distinctive icons that highlight valuable information. Here's a brief overview of what to look out for:

REMEMBER

The Remember icon highlights the importance of a particular idea. This is a great place to use a highlighter, scribble a note in the margin, or bookmark the page for future reference.

TIP

Tips provide concise information that you can use to inform your own exploration of risk management processes.

WARNING

Warnings bring to light practical guidance to help you steer clear of potential pitfalls, costly errors, or frustrating missteps, similar to what you might learn from an experienced veteran in the risk management field.

Beyond the Book

This book lays a solid foundation for understanding risk appetite, managing risk, and, ultimately, achieving organizational objectives. From our executive leadership to our global teams, Protecht has more than 25 years' experience as leaders and practitioners in risk management. Visit `protechtgroup.com` to access additional articles and information, case studies, and white papers that will help you better understand the world of enterprise risk management (ERM). For a comprehensive overview of the technology and services that Protecht provides, check out `protechtgroup.com/dummies`.

By utilizing the information in this book and the extensive resources available through Protecht, you'll be in a great position to improve the risk posture of your own organization with a modern and data-driven approach to understanding, quantifying, and addressing risk.

IN THIS CHAPTER

» Exploring the basic terms and principles of risk appetite

» Integrating risk appetite and risk principles into your organization

» Ensuring that risk appetite is incorporated into enterprise risk management

Chapter 1
Understanding Risk Appetite

In this chapter, you'll explore the core concepts of risk appetite within the framework of enterprise risk management (ERM). You'll discover key terms and then explore how risk appetite integrates into ERM so that your risk management efforts align with your organization's strategic and operational objectives.

Defining Risk Appetite

Risk appetite can be defined as the amount of risk that an organization is willing to accept in pursuit of its goals. It serves as a crucial management tool for organizations, guiding strategies, risk management policies, and all other management tools that provide boundaries for behavior and decision-making. Although all organizations have a risk appetite, many do not formally articulate it — it's driven by convention, managers' preferences, and "unwritten rules." By formally setting a risk appetite, your organization clearly establishes the risks it will pursue, avoid, or accept, ensuring that all levels of decision-making are aligned with the overall strategic objectives and requirements of the highest governing body. For simplicity, when we talk about risk appetite in the rest of this book, we'll be referring to a formally stated risk appetite rather than an implied risk appetite.

TIP

Think of risk appetite as a practical reference point for daily decision-making, risk assessment, and strategic planning.

The key benefits of establishing a risk appetite include:

- **Enhanced decision-making:** Provides a clear framework for making decisions that align with business objectives.
- **Improved resource allocation:** Identifies where risk-taking is most likely to lead to innovation and competitive advantage.
- **Strengthened risk culture:** Sets clear expectations, fostering a risk-aware culture throughout an organization.

Getting a Handle on Key Risk Appetite Principles

Understanding the terminology and principles of risk appetite is essential for leaders who aim to embed risk management as a practical tool that influences all decisions and actions.

The international standard ISO 31000 defines risk as "the effect of uncertainty on objectives." You can find out more about the ISO 31000 standard at `iso.org`. Risk appetite therefore ultimately sets the degree you are willing to accept uncertainty around the achievement of your objectives.

The way we consider risk in this book is based around the preceding ISO definition. The key definitions used in this book are:

- **Risk:** The effect of uncertainty on objectives.
- **Risk appetite:** The degree of risk that the organization is prepared to accept in pursuit of its strategic and operational objectives, expressed in qualitative terms.

- **Risk appetite statement (RAS):** A formal written expression of the organization's appetite for risk, often including both qualitative and quantitative measures.
- **Risk tolerance:** The degree of risk that the organization is willing to accept in pursuit of its strategic objectives and business plans, expressed in quantitative terms.
- **Risk capacity:** The maximum amount of risk an organization can sustain before it impacts its viability.

You may also want to take note of some underlying risk principles, since these will govern much of your thinking as you develop your organization's risk appetite:

- **Strategic enabler:** Risk appetite must inform the organization's strategy and objectives, ensuring a consistent approach to risk-taking.
- **Dynamic nature:** An organization's risk appetite is not static; it evolves with changes in external conditions and strategic priorities.
- **Balance:** Risk appetite should occupy the middle ground between being overly cautious, which can stifle innovation, and being overly aggressive, which can lead to unsustainable risks.
- **Communication:** Risk appetite needs to be clearly communicated across all levels of an organization.

REMEMBER

Setting the right risk appetite for your organization is about finding the sweet spot where risk-taking aligns with your strategic goals without compromising your core values or stability.

Incorporating Risk Appetite into Enterprise Risk Management

ERM is a framework that facilitates the identification, assessment, management, and monitoring of risks across an organization. (Another acronym commonly used for this business practice is GRC: governance, risk, and compliance.)

Risk appetite should be an integral component of an ERM framework. The following are the key eight steps of good risk management from the ISO 31000 risk management standard:

- **Communication and consultation:** This requires engagement with the organization's key internal and external stakeholders to understand the level of risk they are willing to accept as a stakeholder.
- **Scope, context, and criteria:** This identifies the key strategic and operational objectives for which the appetite for uncertainty is being set and the setting of an internal risk appetite, taking into account stakeholders' views.
- **Risk identification:** Identifying the risk that could affect objectives and for which appetite needs to be set.
- **Risk analysis:** Understanding the risk and assessing its size.
- **Risk evaluation:** Evaluating the size of the risk against risk appetite.
- **Risk treatment:** Taking steps to reduce risk if it is outside of appetite.
- **Monitoring and review:** Building the above steps into day-to-day management.
- **Recording and reporting:** Recording the above steps and reporting to stakeholders as to the level of risk against risk appetite.

Risk appetite guides managers and leaders as they determine which risks are acceptable, and which risks exceed their organization's defined risk tolerance levels.

IN THIS CHAPTER

» Setting responsibilities for risk appetite ownership

» Balancing risk with potential rewards

» Determining the inputs into your risk appetite statement

» Setting the right risk appetite levels

Chapter 2
Setting the Right Risk Appetite for Your Business

This chapter explores the relationship between risks and objectives, the importance of setting risk appetite both for objectives and risks, and the critical role of key performance indicators (KPIs) and key risk indicators (KRIs) when creating your risk appetite statement (RAS).

A *KPI* measures how effectively an organization is achieving its strategic and operational objectives, reflecting the reward side of the equation. A *KRI*, on the other hand, signals the risks that may undermine the achievement of the objectives.

Both are essential to clearly stating your risk appetite.

Building Organizational Accountability for Risk Appetite

To incorporate risk appetite into your management practices and culture, you need to clearly set out the responsibilities for risks within the organization. A risk appetite statement (see Chapter 3) acts as a guiding star for the entire organization, influencing decision-making at every level.

Ownership of risk is distributed across various levels:

- **Board of directors:** The board sets the tone and owns the overarching risk appetite.
- **Executives:** Senior executives pursue strategic and operational objectives while managing risks within risk appetite. They are also responsible for the implementation and operation of risk appetite.
- **Risk management function:** This function monitors the application of risk appetite. In some organizations, this may be integrated with the compliance function.
- **Everyone in the organization:** *All employees* are responsible for using risk appetite and ensuring their decisions and behaviors remain within appetite.

Articulating Risk Appetite

Setting the right level of risk appetite guides your organization's approach to setting strategy, objectives, and risk-taking. It requires a blend of clarity, foresight, and practicality. A well-articulated risk appetite forms the cornerstone of an organization's risk management framework and should influence every decision and action.

Determining the appropriate levels of risk appetite is a balancing act that weighs potential rewards against the levels of risk. In this context, you need to consider risk appetite both in terms of objectives (acceptable variation around performance) and risks (which could lead to poor performance). This gives you both a leading view of risk appetite using risks, and a lagging view of risk appetite using objectives.

Balancing risk and reward

The essence of setting risk appetite lies in the balance between the risk an organization is willing to take and the reward it hopes to gain. Taking too little risk may lead to missed opportunities, while taking too much can threaten your viability.

In this context, you should:

- Evaluate potential gains against the level of related risk realization.
- Determine whether potential upsides justify the additional risks, especially when considering strategic decisions such as market expansion or product launches.

Using qualitative and quantitative metrics for risk

A robust risk appetite framework depends on the effective use of both qualitative narratives and quantitative measures to describe risk levels. This approach allows you to have valuable discussions at the highest level using qualitative narratives as well as being able to operationalize the appetite across the business using quantitative measures, which can then be used for ongoing measurement and monitoring of risks against appetite.

Qualitative descriptions humanize the risk data, making it digestible and understandable to every level of the organization. They provide the context behind the numbers, explaining the why and how of risk appetite and risk-taking.

For example, these are qualitative risk statements:

- **Customer satisfaction:** We have a low appetite for uncertainty around our customer satisfaction objective. We aim to maintain the highest levels of customer satisfaction. We will accept a minor decrease in customer satisfaction when launching new products.
- **Business disruption:** We have a low appetite for business disruption. We value a resilient supply chain. Risks that could lead to significant disruption, such as reliance on single-source suppliers, are to be mitigated through diversification.

On the other hand, *quantitative* metrics turn the qualitative concept of risk appetite into concrete, measurable targets. These metrics act as guardrails, guiding day-to-day operations and strategic decisions.

For example:

- **Funding risk:** Maximum tolerance of a 50 percent debt to equity ratio with a warning trigger of 45 percent.
- **Technology risk:** Maximum critical system downtime of 0.8 percent (99.2 percent uptime) with a warning trigger of 0.5 percent (99.5 percent uptime).

Determining the Inputs for Your Risk Appetite Statement

The creation of a RAS (see Chapter 3) is a detailed process that combines your organization's objectives and the related risks.

Defining strategic and operational objectives

You should define two distinct sets of objectives for your organization: strategic and operational.

- **Strategic objectives:** These are high-level objectives focused on changing the organization, such as increasing market share or launching innovative products. For example, your organization might aim for a 20 percent market share increase by entering new international markets.
- **Operational objectives:** These focus on running the business, such as achieving customer satisfaction ratings, maintaining operational efficiency, and complying with regulations.

Identifying the key risks

Risks to your objectives exist regardless of whether you have a formal RAS in place. The RAS defines your willingness to accept them and the thresholds at which you need to take action. You'll need to know and agree on your key risks before writing your RAS as these risks will be the ones you articulate your appetite for.

TIP

Conduct thorough risk assessments regularly to identify new key risks or updates to those you already have identified.

Integrating KPIs and KRIs

KPIs and KRIs serve as the metrics that track the alignment of an organization's performance and risk with its appetite. They need to be carefully defined and integrated.

- For KPIs, identify metrics that directly correlate with strategic and operational objectives, such as revenue growth, market share, customer satisfaction, or operational efficiency.
- For KRIs, select metrics that indicate emerging risks or trends leading to risk events, such as increasing staff turnover, forecasted supply chain delays, or rising debt levels.

Once identified, you'll need to track and report on these indicators. To do this effectively, you should implement a system that captures real-time metric information. For example, you might use data collection tools that feed into an analytics dashboard, providing constant updates on key metrics and highlighting trends that require attention.

Regular reporting intervals should be established, with comprehensive reviews in the context of your organization's objectives and risk landscape, ensuring that stakeholders are kept informed and prepared to act on the insights provided.

TIP

Good enterprise risk management software can automate the data collection, evaluation, and reporting process.

Setting appetite levels

The level of risk appetite will differ across the different types of risks. While strategic risks can warrant a higher appetite for greater rewards, operational risks typically have a lower tolerance due to their potential to disrupt daily activities, and compliance risks may well be set at zero or very low. For example, a company may be willing to risk a certain level of investment in a new project but maintain a strict policy against any breaches in customer data security.

If you want to quantify your appetite for each risk, evaluation zones and thresholds are critical (see Chapter 3).

Understanding indicator evaluation zones

An *evaluation zone* is a means to quickly determine the status of a current risk with reference to appetite. These are often categorized like a stoplight — green, yellow, and red — and help you to readily visualize and thus monitor risks. Table 2-1 provides examples of each of these risk evaluation zones.

TABLE 2-1 Example Risk Evaluation Zones

Zone	Meaning and required escalation and response
Green	Within appetite, no action required. No escalation or specific response required. Non-urgent consideration may be given to assessing reward against risk and ensuring balance is right for risks and rewards in this zone.
Yellow	Within appetite, raised attention. Escalation to board as part of the board reporting process together with an explanation as to why the risk and/or reward is in yellow. Consideration to be given by the board as to ongoing acceptance of risk in yellow or direction to reduce to green, dependent on the balance between risk and reward.
Red	Outside of appetite, action required. Escalation to executive management team immediately and escalation to board latest at the next meeting or earlier as decided by the executive management team. Actions required to be formulated to achieve at least yellow as soon as possible.

These zones can be qualitative assessments or they can be based on metrics with thresholds. The former involves making a judgment to allocate a zone. For example, if you measure risks qualitatively using a risk matrix, you can compare your risk appetite against the risk rating to allocate it to an evaluation zone. In general, the most appropriate use of qualitative or quantitative measures to determine evaluation zones is more of an art than a science, and depends on your personal perspective and the individual risks being assessed.

IN THIS CHAPTER

» Crafting risk boundaries

» Understanding your risk appetite and tolerance for risks

» Writing your risk appetite statement

» Keeping your risk appetite up to date

Chapter 3
Creating Your Risk Appetite Statement

A business strategy often begins with a statement of goals, a starting point that connects objectives to a vision. The same can be said for risk. Organizations start their risk journey by defining a clear and actionable risk appetite statement (RAS).

This process is about defining clear parameters for risk-taking that align with strategic and operational objectives, and then ensuring that every level of the organization understands and operates within these boundaries. You'll discover how to articulate tolerances, set appropriate thresholds for action, and integrate risk management into routine business decisions.

Crafting a Meaningful Risk Appetite Statement

A *risk appetite statement*, or RAS, is not a policy document, but a strategic tool that communicates how an organization evaluates and deals with risk. A RAS should provide direction, facilitate decision-making, and ensure that all activities are aligned with the overall risk strategy. A good RAS is characterized by clarity, relevance, and actionability:

- **Clarity:** Your RAS must be easily understandable, avoiding technical jargon that could obscure its message. Every stakeholder, from the boardroom to the operational level, should understand the boundaries set by your RAS.
- **Relevance:** Your RAS must reflect the current and future market environment, your organization's strategic direction, and its operational context.
- **Actionability:** Your RAS must define specific risk thresholds and what actions are required when these thresholds are reached.

For each key risk or objective, you should have the following:

- **A statement of appetite:** "We have a low appetite for customer satisfaction objectives. We prioritize customer trust, aiming to sustain a high satisfaction rate."
- **One or more measures (qualitative or quantitative) associated with the objectives or risks:** "We track our customer retention rate as a percentage of total customers at start of year."
- **Where relevant, thresholds related to the metrics:** "Our target is a 90 percent customer retention rate. A dip below an 85 percent customer retention rate will trigger an immediate review and response."

When you define these statements in detail, the RAS becomes a document that not only sets the boundaries for risk-taking but also integrates risk management into the strategic and operational processes of your organization.

Setting the Overall Levels in Your Risk Appetite Statement

Creating a comprehensive RAS involves setting appetite levels and tolerances for both objectives and risks. This is where strategic planning meets practical risk management. Let's break down how to set these levels effectively.

Setting appetite and tolerances for objectives

The key to setting appetites for objectives is to clearly identify and articulate your strategic and operational objectives. This step ensures that your risk-taking is in sync with what you aim to achieve.

For each strategic and operational objective, identify the measures of success (key performance indicators, or KPIs) and the targets you have for each of these. For example, if your goal is to increase market share, define what success looks like — is it a 10 percent increase over the next year?

Next, align your risk appetite with these quantified objectives. Consider how much variation you are willing to accept. Articulate that first by using a qualitative "appetite" such as zero, low, medium, or high. If your target is 10 percent market share increase, will 8 percent still be acceptable? Would less than 5 percent warrant a complete strategic review? And do these threshold levels reflect the stated appetite?

TIP

Categorize your risks using the green-yellow-red indicator evaluation zones discussed in Chapter 2.

Setting appetite and tolerances for risks

Setting risk appetites and tolerances can be tricky. There must be an agreed consensus across the highest governing body, where a range of different view will usually abound. It's about finding the right balance between being overly cautious and recklessly daring while ensuring a focus on the achievement of strategic and operational objectives.

When setting appetites and thresholds, the debate must cover the following considerations.

- The tradeoff between risk and reward. You typically cannot have low risk and high reward.
- The tradeoff between risk and cost. The lower the risk appetite, the greater the cost in controlling that risk.

- The implications of setting a risk appetite different to the current level of risk. For example, where the risk appetite is set lower than where the current risk level is, there must be a willingness to either invest more in risk treatment and controls or a willingness to achieve a lower reward.

TIP

Don't try to standardize your threshold levels too much. Some may be decreases and measured in percentage; others can be absolute numbers.

Writing the risk appetite statement

There is no single correct approach to setting out a RAS, and we would encourage you to experiment with what works best for your business. However, we do have some examples to share of what we would consider to be good practice.

- Clarifying the purpose and content of the RAS, plus an overview of the strategic plan, business plan, and related objectives.
- Listing the key risks for which risk appetite will be set.
- Determining the zones and levels to be used to articulate qualitative risk appetite and evaluate quantitative risk tolerance.
- Assessing the qualitative risk appetite for each objective using the qualitative risk scales (for example, zero/low/medium/high) to articulate the level of variation you are willing to accept regarding each objective.

  For example: "Customer satisfaction: Low. We will only accept minimal variation on the downside for customer satisfaction levels" but "Profit: High. We are willing to accept a wide variation to the profit target because we are trying new markets and new innovations which are untested."
- Listing the KPIs linked to objectives and the thresholds for these KPIs using the evaluation zones. You must set the green-to-yellow and yellow-to-red thresholds.
- Setting the qualitative risk appetite (for example, zero/low/medium/high) for each key risk.

For example: “Compliance Risk: Zero” implies you are not willing to accept any compliance breaches, whereas “Strategic Risk: High” implies you are willing to trade off greater innovation for an increased risk of strategy failure.

- Listing the key risk indicators (KRIs) linked to each key risk and thresholds for KRIs using red/yellow/green zoning. You again need to set the green-to-yellow and yellow-to-red thresholds.

Table 3-1 provides some indicative examples of how to complete your RAS.

TABLE 3-1 **Examples of Appetite and Tolerance for Key Risks in Your RAS**

Risk	Measurables	Appetite	Green to yellow	Yellow to red
Market risk	Unhedged FX positions	Low	USD$1 million	USD$1.5 million
Technology risk	% of systems near end of life	Medium	10%	20%
	System outages	Medium	2% per month	4% per month
Cyber risk	Number of successful intrusions	Low	1	2
HR	Unforced staff turnover	Medium	15%	22%
Strategic decision risk	% of strategy decisions aborted after made	High	20%	30%

Adjusting Your Risk Appetite as Your Business Evolves

Even if you select the most appropriate benchmarks, and set your KPIs and KRIs accordingly, you will still need to make modifications over time. A static RAS can quickly become obsolete in a dynamic market environment.

To ensure that your organization's risk approach remains relevant and aligned with its strategic objectives, you need to continuously evaluate and adapt.

A RAS should be reviewed and updated regularly to reflect changes in the organization's objectives, market conditions, or risk landscape. To start, you should:

- Conduct a formal review of the RAS at least annually.
- Align reviews with the rest of your organization's strategic planning cycles.
- Ensure that any changes in business strategy are adequately reflected in your risk appetite.
- Consider the changing expectations of stakeholders.

The review process should involve the same collaborative work between stakeholders as defining the RAS in the first place (refer to Chapter 2).

IN THIS CHAPTER

» Keeping staff and managers engaged with risk appetite

» Operationalizing your risk appetite statement across the organization

» Using risk appetite to make decisions, guide behavior, and form the basis of risk reporting

Chapter 4
Embedding and Using Risk Appetite Across Your Business

This chapter outlines the key strategies for using your organization's risk appetite statement (RAS) across the business. You'll find out how to communicate your RAS effectively, ensure it is integrated into daily operations, and build a robust risk reporting process.

Engaging Stakeholders in the Risk Appetite Process

For a RAS to resonate across an organization, it must be actively embraced by all stakeholders. Achieving this level of engagement means moving beyond a mere presentation to meaningful interactions.

Here are some proven approaches to securing that crucial engagement:

- **Interactive workshops:** Conduct workshops that bring together cross-functional teams to discuss your RAS. Create scenarios where stakeholders can see the impact of risk appetite on their specific areas of responsibility.
- **Feedback loops:** Encourage and incorporate feedback. Show how stakeholder input shapes the RAS, reinforcing their value in the process.
- **Regular updates:** Keep stakeholders in the loop with regular updates about how your RAS influences decisions about business objectives and strategy. This transparency shows the RAS in action and helps validate stakeholder contributions.
- **Success stories:** Share real examples of how your RAS has guided successful results. This not only showcases its effectiveness but also demonstrates practical applications.
- **Communication:** Communicate the RAS to all levels of the organization in a manner that is fit for purpose.

REMEMBER

Inclusivity is key! Ensure your process includes voices from all levels of your organization.

By investing time in these engagement strategies, you build a shared sense of ownership of risk appetite. Stakeholders become active participants in shaping and upholding the organization's approach to risk.

Articulating Your Risk Appetite Across Your Business

Articulating the RAS across your organization requires more than just the circulation of a document. It's about articulating the RAS in meaningful and relatable terms so that it can be made easily understood by all levels of the organization.

You can achieve this with artifacts including:

- Policies and procedures
- Codes of conduct

- Values and commitments
- Minimum control standards
- Cascading risk metrics

It is also useful to use real-life scenarios to show how the RAS applies to different situations across different departments.

Here are some examples:

- Our financial team mitigates credit risk by limiting single-client credit exposure to no more than 5 percent of our total receivables.
- The operations department manages supply chain disruptions by keeping a diversified supplier base in line with our RAS.
- Our IT department applies our RAS by enforcing strict access controls and conducting regular system audits, making sure we comply with our cyber risk thresholds.
- Our sales teams align with the RAS by qualifying leads through a risk assessment matrix, and then focusing efforts on prospects that meet our risk-to-reward criteria.

REMEMBER

Clarity in communication breeds confidence in action. When people understand the why and how of risk appetite — they're more likely to embrace it in their daily roles.

Using risk metrics

One of the best techniques to flow the RAS seamlessly from the C-suite to front-line staff, and ensure alignment with the objectives and key performance indicators (KPIs) of every team, is to use metrics. This allows the collection and analysis of data across the organization, which can be aggregated up to each management level. It ensures that there is one source of truth, that risk evaluation is appropriate for each level of the organization, and that the RAS is cascaded through the organization (see Figure 4-1).

Here are two good ways to ensure that everyone in your organization engages with your RAS:

- **Tailor your metrics:** Use a combination of metrics that are needed to be aggregated up to management level, supported by specific metrics for each department that are relevant and staff can relate to and manage.

- **Provide consistent messaging:** While your metrics can be tailored to different departments, your overall message needs to be uniform across your organization. Use recurring, broad briefings — such as in quarterly business reviews — to reinforce how your RAS applies to your employees to improve contextual understanding.

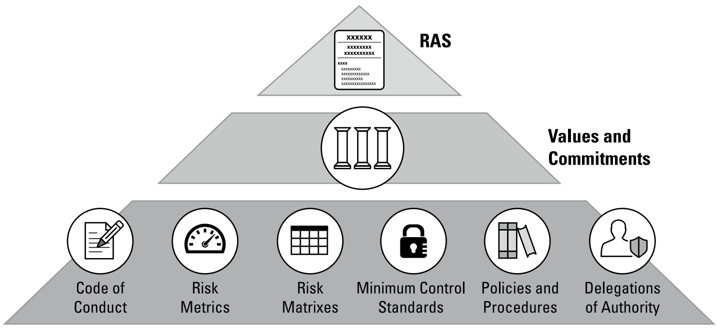

FIGURE 4-1: Cascading and operationalizing the RAS throughout an organization.

Pushing the RAS through management to individual contributors

Your management team must act as the conduit for your RAS, ensuring it reaches every employee in a meaningful way. This is where the RAS transforms from a strategic concept into a practical guide for daily decisions.

You should have regular meetings and activities that demonstrate how the RAS impacts daily routines. It needs to be a part of the fabric of your company. Then, celebrate the wins! Call out activities that use your RAS to drive successful outcomes. For example:

- Spotlight a team that preemptively mitigates a risk that could have thrown off project timelines, using the RAS to identify the problem.
- Recognize an individual who identifies a planned behavior as being outside of appetite and calls it out to ensure that behaviour is modified.

- Give a shout-out to a department that has used its increased risk appetite to achieve greater reward while managing the increased risk well.

REMEMBER

Not all decisions lead to good outcomes — but that doesn't mean the decision was a bad one. Every decision includes uncertainty. Celebrate people who take smart, well-informed risks, and scrutinise less informed decisions where someone simply "got lucky."

Making sure your communication is working

Finally, you have to work to ensure that your communication is received well. It's not enough to have a great communication strategy if your message isn't landing with your teams. You must establish mechanisms to confirm that the message is not only heard but also acted upon.

The easiest approach here is often the most effective: Solicit feedback early and often. Encourage your teams to discuss the RAS and your risk appetite in meetings, all-hands sessions, and 1:1 discussions.

The more you hear risk appetite discussed, and the more people offer their opinions and insights, the more your communication techniques are working.

Reporting Against Risk Appetite

The RAS should be used as a basis for robust risk/reward-based reporting. In particular, the use of metrics to track both outcomes and risks together with related measurement thresholds, allows risk/reward reporting that evaluates rewards and risks against the stated risk appetite.

To ensure your reporting supports your risk appetite, you should:

- **Establish clear metrics:** Use the KPIs and KRIs (key risk indicators) that you have set up in your RAS as the metrics that you track over time.
- **Report both risks and rewards together:** KPIs provide insight into performance against objectives and KRIs provide

insight into the level of risk being taken to achieve the objectives.

- **Integrate into existing reports:** Incorporate risk appetite metrics into regular management and performance reports to ensure visibility.
- **Automate for consistency:** Utilize risk management software to automate the collection and reporting of risk data, ensuring accuracy and timeliness.

Driving Decision-Making with Risk Appetite and Risk Reporting

A key use of risk appetite and related reporting is to assist in better and more timely decision-making. Here's how risk appetite and reporting should guide you:

- **Risk appetite boundaries determine whether you "can" or "should" (the "Can I/Should I" test):** When decisions are being made, an assessment should be made as to whether the risks expected to arise from the decision are within or outside of appetite. This is known as the "Can I?" test. Where the risks are outside of appetite, you cannot, no matter what the reward may be. Where they are within appetite, you can. For those that you "can," you assess the risk level against the reward level to assess whether you "should." Here, you select the option where the reward exceeds the risk and provides the best reward-to-risk trade-off.
- **Reports provide assurance:** Your reports give you a clear yes or no on whether you're within your risk appetite. This can give you the confidence to pursue more business opportunities.
- **Reports raise red and yellow flags:** Red flags should drive you to take immediate action to get back within appetite, while yellow flags make clear when you're close to the edge of your appetite for closer scrutiny.

TIP

If you can easily think of key decisions that were affected by your risk reporting and appetite, that's a good sign that you are using risk appetite to drive decision-making.

IN THIS CHAPTER

» Aligning metrics with strategic objectives

» Embedding risk appetite into management processes

» Ensuring risk appetite is used day-to-day by staff at all levels

» Using the right business processes and software solutions to support risk appetite

Chapter 5
Ten Tips for Effective Risk Appetite Management

As you evolve your risk appetite in your own organization and learn to apply it over time, you'll want to avoid common mistakes. Here are ten tips that will help you develop an effective risk appetite.

REMEMBER

You won't necessarily be able to absorb and apply all these tips at once. However, you can pick one or two to focus on, and then return to this chapter as your organization grows and evolves, continuing to add additional enhancements.

Link Risk Appetite to Your Strategy and Business Plan

Ensure that your RAS is not an isolated document but is an integral part of your overall business strategy and plan. This alignment guarantees that risk-taking is always in service of your organization's broader goals.

REMEMBER

Regularly align your RAS with any changes in business strategy to maintain relevance and effectiveness in your risk management approach.

Ensure Trade-offs between Risk and Reward Are Clearly Understood

When risk appetite is set, it should not be set in isolation. It must be set with full appreciation of the trade-off with reward and/or cost.

For example, if risk appetites are set very low, this may lead to a reduction in reward and/or an increase in cost to manage that risk. If risk appetite is set too high, this may create more opportunity and reduce the cost of control, but there should be an expectation of more things going wrong and risk incidents occurring.

Make Risk Appetite Part of Management

Integrating risk appetite into daily management decisions helps embed a risk-aware culture. Managers should be equipped and enabled to make decisions that reflect the organization's risk preferences, using the risk appetite statement (RAS) as a guide in their operational choices and strategic planning.

TIP

Regular training for managers on interpreting and applying the RAS can significantly enhance its integration into decision-making.

Design Risk Appetite to Encourage Appropriate Action

Frame your risk appetite to not just prevent excessive risk-taking but also to encourage calculated risks where appropriate. A well-designed risk appetite provides freedom within boundaries. This helps foster innovation and growth, as long as the risks are within the defined appetite and contribute to strategic and operational objectives.

Articulate Risk Appetite in Clear and Understandable Language

As risk appetite provides boundaries within which all staff should operate, it needs to be easily understood and communicated across the whole business.

Language used should be in line with everyday language, and metrics used for tolerances must be legitimized and able to be applied.

This means that appetite should be communicated in a wide variety of ways that are relevant for the audience, including metrics, statements, and values.

Define Accountability and Action for Risks Outside of Appetite

Establish clear guidelines and responsibilities for actions when risks fall outside the organization's risk appetite. This includes identifying who is responsible for what actions and ensuring that there are predefined plans to address these risks.

WARNING

Clearly define escalation procedures for risks that exceed tolerance levels to ensure timely and effective responses.

Set the Right Metrics

Setting the right metrics is a cornerstone of effective risk appetite management. These metrics need to be closely aligned with both your strategic and operational objectives and key risks. Well-chosen metrics can provide early warning signals and ensure risk evaluation and related decision-making is proactive, not reactive.

Financial metrics might include variations in cash flow with defined thresholds, whereas in a project management scenario, it could be deviations from project scope, timelines, or budget.

In addition, as the metrics will be reported at different levels of the organization, the metrics must be at the right level. Management metrics will not be relevant to a board, and equally board metrics may be too high-level for management.

Structure Reporting to Get Data to All Levels of the Organization

Develop a clear reporting structure that allows risk information (mainly risk metrics) to flow seamlessly from the ground up. This ensures that critical risk data reaches all levels, enabling comparison against risk appetite and informed decision-making throughout the organization.

WARNING

Avoid information overload. Tailor risk reports to be concise and relevant to each organizational level to maintain clarity and effectiveness.

Review Your Risk Appetite Regularly

The business environment is dynamic, necessitating regular reviews of your risk appetite. This ensures that your risk appetite and related reporting and decision-making are aligned with changing market conditions, regulatory landscapes, and internal strategic and operational priorities.

Use the Right Software System to Embed Risk Appetite Data

Working with your enterprise risk management software provider, aim to develop a clear risk data reporting structure that allows risk information to flow seamlessly from the ground up.

This approach ensures that critical risk data reaches all levels, enabling comparison against risk appetite and informed decision-making throughout the organization. An approach based on shared files or individual spreadsheets cannot provide the enterprise-level view that is essential to understand how you are performing relative to risk appetite.

When evaluating a new or upgraded enterprise risk management software system, make sure that it is able to support enterprise-wide visualization and monitoring of risk appetite.

Define, set, and manage your business's risk appetite

Setting your risk appetite allows your business to find the balance between taking enough risks to grow and taking too many risks to survive. It can be a tricky process — but the rewards of getting this balance right will empower your team at every level to make smart business decisions that deliver. With the information shared in this book, you can improve your business's understanding of risk and reward and implement a data-driven approach to understanding, quantifying, and addressing risk.

Inside…

- Identify objectives and associated risks
- Factor KPIs and KRIs into your plans
- Integrate risk appetite into operations
- Write a future-proof risk appetite statement
- Involve your team with effective comms
- Drive effective decision-making

PROTECHT

David Tattam is co-founder and Chief Research and Content Officer at Protecht. Previously, he was Chief Risk Officer and Head of Operations at two major banks. **Brett McLaughlin** is a 25-year tech veteran, whose experience ranges from working on NASA's cloud data program to CTO roles at Volusion, sticky.io, and Carbon6.

ISBN: 978-1-394-23785-2
Not For Resale

for dummies®
A Wiley Brand