What Is Your Risk Appetite?

Mukul Pareek, CISA, ACA, AICWA, PRM, is a risk professional based in New York, USA. Pareek is the copublisher of the Index of Cyber Security (*cybersecurityindex.org*) and the author of a risk education web site, *www.RiskPrep.com.*

As a risk manager, knowing the organization's risk appetite means knowing how much risk the organization is comfortable bearing. In the financial world, risk appetite is almost always expressed explicitly, in the form of value-at-risk limits, and limits on concentration risk, counterparty exposures, liquidity, leverage and so on. This explicit expression takes the form of money units—dollars and cents, for example—making everything fairly objectively measurable and reportable.

For risk managers responsible for operational risk, such explicit statements of risk appetite are difficult to enunciate. Risk, in these contexts, is often measured in terms of being high, medium or low, or a similar subjective scale, with a great deal of reliance on the risk manager's judgment.

Risk appetite then takes a loosely accepted understanding that the highest-rated risk factors are to be addressed first, but without clearly stating if they are either acceptable or unacceptable for the organization to hold. This is in stark contrast to thresholds for financial risk, where breaching a limit requires almost immediate risk reduction with escalation and communication happening automatically.

CHALLENGE FOR THE TECHNOLOGY RISK MANAGER

For the technology risk manager, the challenge is similar in that clear boundaries for the extent of information-systems-related risk that management is willing to keep are undefined. Explicit statements of risk appetite rarely exist. Decisions on whether to live with a risk or mitigate it are largely based on judgment and, often, on what resourcing and budgetary situations permit in any particular situation. Knowing the organization's risk appetite means being clearly aware of the nature and kinds of risk that are acceptable, those that are unacceptable, and those that are acceptable only after executive review and approval.

> "Explicit statements of risk appetite rarely exist."

SETTING RISK APPETITE IN A TECHNOLOGY RISK CONTEXT

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines risk appetite as "the amount of risk, on a broad level, that an organization is willing to accept in pursuit of value."[1] ISACA defines risk appetite in a similar way as being "the amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission."[2] However, because the *amount of risk* is not a discrete threshold against which a technology risk manager can objectively evaluate individual findings or the risk, a formal approach that states the risk appetite in terms of the risk actually encountered needs to be developed.

Articulating the risk appetite involves setting the standard against which assessed risk is compared with a view to making a decision on avoiding, mitigating or holding risk. But, as ISACA's definition of risk appetite states, risk appetite has relevance only within the context of the organization's mission. The risk that would be acceptable for an organization focused on increasing market share would be different from one that places a higher priority on protecting reputation, which, in turn, would be different from an organization that seeks to provide superior customer service. The business managers involved in codeveloping and setting the risk appetite need to be those whose responsibilities relate directly to the organization's mission and whose business processes IT supports.

Of course, an organization may have multiple objectives, not all of which are equally important. In fact, defining, communicating and gaining acceptance for an explicitly stated risk appetite from business managers can be a great engagement opportunity for the risk manager. Resourcing and funding discussions can also benefit from a focus on whether a given risk exposure is above or below the risk appetite.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

RISK RATINGS AND RISK APPETITE

So how does one express risk appetite? A lazy way may be to relate it to the results of risk assessments. For example, one could express risk appetite as a simplistic statement saying that the organization is comfortable living with risk rated medium or low, but not with risk rated high or critical. The trouble with this approach is that it lacks clarity and specificity, and, therefore, it is open to challenges by business managers and technologists alike. It is not specific because it focuses on a rating that is one level removed from the risk itself and, as an abstraction of the seriousness of the underlying issue, represents the technology risk manager's perspective, which may not be shared by others.

A formal statement of risk appetite should establish the objective scale against which the risk could be measured and compared, and the risk rating determined thereafter. The formal statement of risk appetite could then provide the rationale as to why a particular rating is assigned to a finding, as opposed to the rating determining if the finding falls outside of the acceptable risk threshold.

Risk ratings and rankings are widely used in organizations, yet countless hours spent arguing with auditees on why something should be high instead of medium (or the other way around where the auditee has a self-interest in pushing a pet project) illustrate that such assessments make auditees miss the risk perspective. Further, risk ratings are often disconnected from the organization's purpose and are difficult to act upon, as senior management may not sponsor the efforts required to remediate or address the risk factors classified in this manner. For this reason, issues and findings, even those rated high, tend to live on far longer than they should. Therefore, using risk ratings as the surrogate for expressing risk appetite is not a good idea. This does not mean that the risk rating is no longer relevant, only that it follows and uses the results from a measurement against the statement of risk appetite as one of the inputs in its determination.

Explicitly setting the risk appetite allows the risk manager to state with clarity and authority which kinds of risk are acceptable and which are not. It is then possible to hold accountable groups that are responsible for addressing risk that goes beyond the organization's risk appetite. Decisions are also less open to organizational debate because issues are being measured against agreed criteria, as opposed to being assigned a risk rating that needs to be continually justified and defended.

EXPRESSING RISK APPETITE

So how does a statement of risk appetite manifest itself in a practical way? Is it a lofty statement of good intentions that is high on the acceptance scale, but low in implementation quality? Or is it so detailed that it includes every possible risk that exists in an organization's risk universe? A high-quality statement of risk appetite is probably somewhere in the middle. One way to think about it would be to consider the ways a risk would be realized, and then think about the classifications, attributes or characteristics that the risk realization paths bear. Risk appetite can then be expressed in statements that are clear, are stated in a way that supports protecting the achievement of business objectives and are agreed to by senior management.

Figure 1 provides examples of statements of risk appetite stated in binary terms as being acceptable or not. The examples focus on cybersecurity risk, though the analogy may be extended to other kinds of IT risk, of which cybersecurity risk is a subset. As organizations mature, these statements of risk appetite may be explicitly tied to operational and financial performance objectives. That linkage is not demonstrated in the examples provided in **figure 1** for reasons of brevity, and it is assumed that if a risk is unacceptable, it is because it impacts the organizational objective in an unacceptable manner.

Figure 1—Example Statements of Risk Appetite			
Risk Manifestation	**Asset/ Business Impacted**	**Appetite**	**Action**
Vulnerabilities			
Remote code execution vulnerabilities in technologies hosting customer data	Customer franchise	No appetite	Fix immediately
Vulnerability requiring no authentication to exploit on customer web site	Business reputation	Acceptable with senior management agreement	Prioritize and fix
Vendors			
High-risk data shared with vendor missing baseline data leakage controls	Client franchise	No appetite	Cease business with vendor
Low-risk data shared with vendor missing baseline data leakage controls	Internal data	Acceptable	No action
Applications			
No protection against SQL injection on intranet application	Internal applications	Acceptable	No action
Cross-site scripting vulnerability in Internet-facing customer application	Profitability targets	No appetite	Fix immediately

In the same way, risk appetite could be stated for other technology risk issues; for example, whether or not an IT general control weakness qualifies as a material deficiency could provide the test for the risk being acceptable or unacceptable.

BUILDING ON THE FOUNDATION

Over time, the simplistic risk appetite statements may need to develop into more complex and better stated frameworks that include a number of different, related elements:

1. **The cost of risk avoidance or mitigation**—A missing element in **figure 1** is the question of the cost of risk avoidance or mitigation. What if the medicine is worse than the ailment? For example, what if the business faces an unacceptable level of risk when measured against the stated risk appetite, but the cost of the cure is something the business cannot bear or there are consequences that are equally unacceptable? Clearly, the nature and effects of dealing with the risk need to be considered and incorporated into the statement of risk appetite.
2. **The core risk**—At the most detailed level, there could be at least as many risk factors defined as there are controls. This would make the task of assigning an appetite statement to each of them quite daunting and practically impossible, given that the business environment and, therefore, the controls that organizations adopt as a response are rarely static. What is required is the generalization of the specific risk into a more easily understood and higher-level risk. Continuing the example of cybersecurity risk, risk could be distilled into a handful of factors (such as remote code execution, privilege escalation, denial of service and asset theft) and the organization could have a risk appetite statement for each.
3. **Connection to business objective**—Each risk should have a clear connection to business objectives, which should be clearly brought out as part of stating the core risk. Business objectives could include, for example, profitability, reputation, compliance, cost control and customer experience. These should be discussed with business executives as part of the exercise to formulate the organization's risk appetite.
4. **Graded scale for expressing risk appetite**—While the binary expression of risk appetite illustrated previously may be a good and easy way to get started, it is more of a first step in the process. As managers consciously realize the limits of their risk tolerance, a more nuanced and graded expression of risk appetite, perhaps along a sliding scale, can be put in place. This would include gradations such as "acceptable" on one end of the scale, following through with "reluctant to accept," "averse" and "unacceptable" at the other end.
5. **Authority for risk decision making**—The moment the organization moves to a higher level of maturity than expressing risk appetite on a binary scale, questions of communication and escalation arise. Some of the statements of risk appetite may require submitting the risk for consideration by a named risk decision-making authority, which could be a risk committee or a senior manager. These downstream processes need to be defined as part of managing the risk appetite statement.
6. **Risk aggregation**—Risk may need to be considered together in its totality. What may seem acceptable as a stand-alone

risk may not be acceptable when considered together with other risk factors. The organization's risk appetite may need to make an allowance for considering risk in aggregation in terms of its impact on business objectives.

CONCLUSION

Understanding the need to ascertain and express risk appetite is a task of self-discovery for any organization. It helps crystallize the organization's true attitude toward risk and forces a hard look by senior management at how far it is willing to let the organization walk on the technology risk plank. Risk appetite should answer the question as to which risk factors the organization is comfortable bearing and which it is not. It should transform risk discussions by making irrelevant the likely different interpretations of what is acceptable to live with each time a risk assessment or audit is performed.

To summarize, the following points are worth keeping in mind:

1. In the end, risk appetite is a position adopted by members of senior management in pursuit of their objectives. It is their opinion and point of view, and that is how it should be presented to the rest of the organization—not as a *diktat* from the technology risk manager.
2. Risk appetite is not static. As the risk landscape evolves and the business environment shifts, risk appetite must adjust. The adjustment frequency may be annual or more often, depending on how fast the organization moves and is affected by technology risk.
3. The expression of a risk appetite is not a one-size-fits-all exercise. Frameworks can help, but each organization has to lay down its own path in line with its risk tolerance and decide how formal, detailed and mature its statement of risk appetite should be.
4. If a linkage to the organization's objectives cannot be established because it appears too far-fetched, perhaps the right business executives are yet to be consulted. Technology supports the organization; therefore, its risk appetite must be determined by the organization.
5. When bad things happen in the world of technology, business and executive managers often express surprise. Developing a statement of risk appetite in partnership with business executives can help set expectations, drive engagement and avoid surprises.
6. Risk appetite should be actionable in a way that analysts or auditors working for the technology risk manager can use it as part of their day-to-day battles. It should remove uncertainty on senior management's perspective on issues and findings.
7. Technology risk managers should own and manage the process of setting and communicating risk appetite. In doing so, they should consult with the right groups in their organizations; propose, draft, communicate and revise the statements of risk appetite with senior management; and obtain senior management's approval and authorization.
8. Judgment is critical when laying down risk appetite, and more so when applying it. Risk appetite should provide strong guidance, yet allow judgment to be exercised in situations where management's intent appears to be different.

ENDNOTES

[1] Rittenberg, Larry; Frank Martens; *Thought Leadership in ERM, Enterprise Risk Management, Understanding and Communicating Risk Appetite*, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2012, *www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf*

[2] ISACA, Glossary, Risk Appetite, *www.isaca.org/glossary*