How to Build an Actionable Technology Risk Appetite Framework

Published 21 September 2020 - ID G00719524 - 14 min read

By Analysts Srinath Sampath

Initiatives: IT Cost Optimization, Finance, Risk and Value and 2 more

Organizations struggle to make consistently risk-informed choices about how to prioritize investments, largely because they lack an effective expression of their technology risk appetite. CIOs must partner with business and technology risk leaders to articulate and operationalize this risk appetite.

Overview

Key Challenges

- Most articulations of technology risk appetite are too high level and vague, failing to provide decision makers with actionable guidance.

- Organizations struggle to develop an enterprise-level articulation of risk appetite that can be effectively translated into policies, procedure and metrics to influence day-to-day decision making.

- Technology and risk management leaders end up creating the organization's de facto risk appetite without the necessary and effective input from business leaders.

Recommendations

CIOs responsible for IT cost optimization, finance and integrating risk and corporate performance should:

- Elicit executives’ appetite for technology risk by guiding them through hypothetical/real scenarios and gauging their tolerance for uncertainty in achieving business outcomes due to technology risk issues.

- Ensure the practicality of the executive-articulated risk appetite by soliciting feedback from operational leaders.

- Translate the high-level statements into specific and actionable guidance for decision makers by embedding measurable risk appetite principles into policies, procedures and operational metrics.

- Track the organization's adherence to articulated risk appetite by establishing an ongoing reporting process for escalations and exceptions.
Introduction

Technology risk is an inescapable reality in today’s world, where a large majority of organizations are investing in digital business. All technology risks need not be bad for the organization. For example, organizations do need to take calculated risks when investing in new business models as they try to remain competitive amid continuous disruption by the digital giants and digitally native competitors. At the same time, they want to protect themselves against accepting risks that they aren’t comfortable with, such as unplanned downtime on critical business processes or loss of customer data. Then there are technology risks that aren’t desirable, but may just be part of the organization’s reality, such as technology debt, or misalignment between the technology capabilities and business strategy. Hence, it is extremely important that an organization understand and operationalize how much and what types of technology risk they’re willing and able to accept, so that they can focus their risk management efforts on mitigating the rest.

Risk appetite is a term that many executives — whether in risk management roles or otherwise — use in passing, but not many organizations care to formally articulate their risk appetite. Reasons for this range from the principle of discoverability in a legal context, to the perceived lack of clear benefits, to the nebulousness of the concept. In the Gartner analyst community’s general experience, even when organizations do formally articulate their risk appetite, the result is usually ineffective at informing decision making. But that doesn’t mean it can’t be done in a manner that supports better decision making in a business context. And there are plenty of reasons why organizations should evaluate, discuss, articulate, and operationalize their risk appetite (see Learn Your Risk Appetite or Fail at Risk Management). Two-thirds of the top performing CISOs develop risk appetite statements in partnership with their senior executive stakeholders, compared to only a third of bottom-performing CISOs (see Note 1).

This document assumes that the organization:

- Accepts the value of articulating and operationalizing a technology risk appetite
- Is pushing forward with developing and leveraging risk appetite

Convincing skeptical executives of the need for a formal risk appetite is a milestone in itself. However, a lot of work needs to be done to make it an integral part of how decisions get made within the organization. Figure 1 is an illustration of the typical steps in the process an organization would go through to articulate and operationalize a technology risk framework into business-as-usual decision making.

Figure 1: Illustrative Process Flow for Implementing a Technology Risk Appetite Framework
Analysis

Elicit Senior Stakeholders’ Preferences on Technology Risk

The one big mistake that organizations often make is leaving it up to the technology and risk leaders to decide how much technology risk the organization will accept. This often happens because the conversations taking place in the executive suite and the boardroom are focused on the technical aspects of cybersecurity and technology risk. This is evident from the hundreds of board-level and C-suite presentations on technology risk that Gartner analysts review on a regular basis, and the blame has to be shared by both sides:

- CIOs and CISOs along with their teams who continue to communicate risk through a technical lens.
- Business leaders who continue to remain disengaged in the process

The answer is to create a model of shared accountability and responsibility between the risk team and the business, where:

- The risk team effectively sheds a light on business outcomes which are at stake because of technology risk.
- The business leaders articulate their level of tolerance for uncertainty in achieving their objectives.

See Establish Shared Accountability for IT Risk and Toolkit: Board-Ready Slides for Cybersecurity and Technology Risk.
Technology risk appetite should be set by the senior-most leaders of the organization — a C-suite or equivalent. In order to get these executives to elicit their preferences on technology risk appetite, they must understand the business impact of technology risk exposures, so that they can decide the extent to which they would accept those risks in the pursuit of their objectives. To do this, CIOs should build scenarios revolving around the top business outcome impacts resulting from technology risk exposures in the organization's risk register (see Why You Need a Risk Register).

Here are some sample scenarios that can help facilitate the conversation:

- Our organization is slow to invest in digital business models in a quickly transforming industry and we lose significant market share to other incumbents and new digitally native entrants.
- We are hit by a ransomware attack and lose access to our systems and data for an extended period of time, with the attackers demanding $XXXX in bitcoin to decrypt our data.
- We lose thousands of records, including PII on clients and employees, due to a cyberattack on a third party to which we outsource our payroll services.

While the scenarios can go into the root causes of the risk exposure, it’s much more important that they expand on the business impact/consequences of the risk to the organization. It’s also important that executives understand why the organization may want to accept a specific risk, and what it would cost to mitigate the risk if the organization finds it unacceptable. Once this happens, executives can focus on how willing they are to accept a particular risk in the pursuit of their objectives. To mirror real-life situations effectively, there should be multiple scenarios covering best-case, worst-case and most-likely possibilities.

Using the scenarios as reference, CIOs can pose the following questions to the executives to elicit their views on risk acceptance versus avoidance:

- What is our tolerance for uncertainty to our objectives caused by this risk exposure?
- Is there an upside (strategic, operational or financial) to the organization of accepting this risk? Is the upside worth the uncertainty?
- If a specific risk exposure is unacceptable, how much would we be willing to spend to bring it back within an acceptable range?
- What would it cost if we accepted the risk and did nothing to fix it?

These conversations around risk, value and cost must go hand-in-hand for executives to make practical and useful choices around how much risk to take, why, and how to invest organizational resources appropriately (see Optimize Risk, Value and Cost in Cybersecurity and Technology Risk).
The 1-5 scale in Table 1 can help normalize responses from different stakeholders, and help build consensus among them on how they would define the organization's risk appetite on specific exposures. The accompanying questions can help the executives clarify their preferences especially in the context of the inevitable trade-offs they'll be expected to make.

### Table 1: Sample Risk Appetite Rating Scale

<table>
<thead>
<tr>
<th>Rating</th>
<th>Risk-Taking Philosophy</th>
<th>Tolerance for Uncertainty</th>
<th>Choice</th>
<th>Trade-Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 — Open</td>
<td>Will take justified risks</td>
<td>Fully anticipated</td>
<td>Will choose option with highest return; accept possibility of failure</td>
<td>Willing</td>
</tr>
<tr>
<td>4 — Flexible</td>
<td>Will take strongly justified risks</td>
<td>Expect some</td>
<td>Will choose to put at risk; but will manage the impact</td>
<td>Willing under certain conditions</td>
</tr>
<tr>
<td>3 — Cautious</td>
<td>Preference for safe delivery</td>
<td>Limited</td>
<td>Will accept if limited and heavily outweighed by benefits</td>
<td>Prefer to avoid</td>
</tr>
<tr>
<td>2 — Minimalist</td>
<td>Extremely conservative</td>
<td>Low</td>
<td>Will accept only if essential and limited possibility/extent of failure</td>
<td>With extreme reluctance</td>
</tr>
<tr>
<td>1 — Averse</td>
<td>“Scared” — risk avoidance is a core objective</td>
<td>Extremely low</td>
<td>Will select the lowest risk option, always</td>
<td>Never</td>
</tr>
</tbody>
</table>

These questions can help elicit stakeholders' perspectives on acceptable levels of risk exposure.

Source: Gartner

Going through this exercise will help the organization land on a high-level articulation of technology risk appetite from the perspective of the senior executives. CIOs should think about this
risk appetite statement as similar to commander's intent, which is a military concept.

Commander's intent is a publicly stated description of the end state as it relates to forces (entities, people) and terrain, the purpose of the operation and key tasks to accomplish.

Gather Feedback on Draft Risk Appetite Statements From Operational Leaders

One of the biggest pitfalls that risk appetite statements suffer is that senior executives articulate a formal statement without taking inputs from or communicating with people in operational roles — those regularly making decisions that ought to be influenced by the risk appetite. This is one big reason why risk appetite statements often end up as paper weights that don’t get operationalized into the governance and decision making of an organization. Based on Gartner research into what factors drive the alignment of decision making with articulated risk appetite, the following things matter the most, in ascending order of importance:

1. Knowledge/awareness of the risk appetite
2. Specific guidance on how the stated risk appetite applies in a particular case
3. Consistency of the stated risk appetite with other messages and priorities

CIOs must gather feedback from individuals in operational roles to understand how practical and useful the senior leaders’ articulations on risk appetite are when it comes to decision making (see Figure 2). The following questions can help test for the perceived relevance and practicality of the draft statements among operational leaders:

- Does the statement give you a clear understanding of the organization’s posture toward risk taking?
- Based on the statement, is it clear to you how the organization expects you to make decisions?
- Can you realistically base your decisions on the stated risk appetite on a consistent basis?
- Is the statement consistent with other messages — both explicit and implicit — you receive from your leaders and peers that affect your decisions?

Figure 2: Feedback Loop Between Executive Leaders and Operational Management
It can take a few iterations of feedback and rearticulation to get the verbiage and sentiment of the high-level statement in a place where everybody is comfortable with it. But it is definitely worth the effort if the organization wants the risk appetite framework to be a useful tool in the decision-making process.

**Operationalize Articulated Risk Appetite Into Business-as-Usual Practices**

Once the high-level risk appetite statement has been articulated and approved by the senior executives, the tough work begins of merging the desired risk appetite into standard operating procedures, risk treatment plans and risk metrics.

CIOs should direct their teams to conduct a review of their existing policies that affect technology risk management — including information security, business continuity and vendor management — to ensure that the policies align with the articulated risk appetite. The organization will also need to ensure that all stages of the technology risk management process — including risk assessment, treatment planning and reporting — are explicitly aligned with the stated risk appetite.

To embed technology risk appetite into metrics, organizations will have to rely on a combination of historical values, industry standards and subject matter expertise/judgment to come up with thresholds. First and foremost, organizations will need to ensure that they are identifying and
tracking leading indicators of risk exposure instead of just measuring the losses and consequences of failure (see Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making). Next, the organization will need to establish some thresholds on the metrics to drive action when exceeded.

For example, if phishing click-through rates are a leading indicator of the risk of data breaches (for which the organization has articulated a low appetite), the organization will need to decide where to draw the line on click-through rates. Is 40% too high? Is 10% achievable? In the absence of true quantification of the impact of reduction in click-through rates on loss expectancy, organizations will have to rely on judgment and benchmarks to establish thresholds for themselves. See Outcome-Driven Metrics for Cybersecurity in the Digital Era and How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation.

Set Up a Risk Appetite Exception and Escalation Process

If there's a specific business need for which the organization needs to operate outside previously articulated risk appetite, there needs to be a formal process through which such exceptions can be raised. Ideally, this should be brought to the attention of the cyber steering committee so that a decision can be made about whether:

- A one-off exception is to be made.
- A change in the organization's risk appetite ought to be recommended.

The reasons for the exception being requested should be clearly documented. Also, the organization should state whether the exception is temporary, and if so, under what circumstances it will be revoked or rescinded.

Conclusion

Risk appetite is an often misunderstood concept, but it can be a very helpful framework to consistently align decision making with the senior leadership’s preferences toward risk taking. This ensures that organizations:

- Take the risks that they need in order to achieve their objectives — e.g., investing in bold digital initiatives to capture market share in an evolving industry.
- Avoid or minimize the risks that mostly/exclusively have downsides — e.g., unplanned downtime on critical business processes, loss of critical information assets.

It is important for CIOs to ensure that the conversation on technology risk appetite is framed in the right context. For senior executives who should be setting the risk appetite for the organization, the context should focus on impact on business processes and business outcomes. For the
technology and risk leaders who will ultimately operationalize the risk appetite, the context should be on operational outcomes and root causes of risk exposures.

**Note 1: CISO Performance**

![Figure 3: Top-Third-Performing CISOs’ Proposed Changes in Time Allocation](image)

**Prevalence of Behaviors Among CISOs by Performance**

Percentage of Bottom Third and Top Third Performers Exhibiting Each Behavior

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Bottom Third (n = 43)</th>
<th>Top Third (n = 44)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate Discussions on Evolving Norms to Stay Ahead of Threats</td>
<td>80%</td>
<td>37%</td>
</tr>
<tr>
<td>Prioritize Keeping Decision-Makers Aware of Current and Potential Future Risks to the Enterprise</td>
<td>56%</td>
<td>61%</td>
</tr>
<tr>
<td>Proactively Engage in Securing Emerging Technologies</td>
<td>70%</td>
<td>61%</td>
</tr>
<tr>
<td>Have a Formal and Actionable Succession Plan</td>
<td>35%</td>
<td>37%</td>
</tr>
<tr>
<td>Define Risk Appetite Through Collaboration With Senior Business Decision-Makers</td>
<td>66%</td>
<td>37%</td>
</tr>
</tbody>
</table>

n = 129 CISOs

Source: 2020 Gartner CISO Effectiveness Survey

Note: Percentage point difference may be slightly different from the gap between the top and bottom third due to rounding.

728433_C

**Recommended by the Author**

**Optimize Risk, Value and Cost in Cybersecurity and Technology Risk**

**Establish Shared Accountability for IT Risk**

**Toolkit: Board-Ready Slides for Cybersecurity and Technology Risk**

**Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making**

**Outcome-Driven Metrics for Cybersecurity in the Digital Era**

**How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation**

**The Urgency to Treat Cybersecurity as a Business Decision**
Recommended For You

Summary Translation: Jump-Start Your Innovation Journey With a Customizable Innovation Framework
8 KPIs That Demonstrate How Self-Service Initiatives Advance Your IT Service Desk
Critical Steps for Tech Product Managers: Invest in the Right Tools
Magic Quadrant for Full Life Cycle API Management
Market Guide for Integrated HR Service Management Solutions

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."