

How to Articulate an Actionable Risk Appetite

Jim Fitzmaurice
VP, Advisory

© 2024 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."](#)

Gartner®

Alligator vs. Shark



Key Issues

1. Risk appetite needs to be actionable
2. How to make risk appetite statements actionable
3. Ensure better buy-in to the risk appetite by the business



Key Issues

1. Risk appetite needs to be actionable
2. How to make risk appetite statements actionable
3. Ensure better buy-in to the risk appetite by the business





Decisions about strategic initiatives are too often misaligned with leadership's risk-taking preferences.

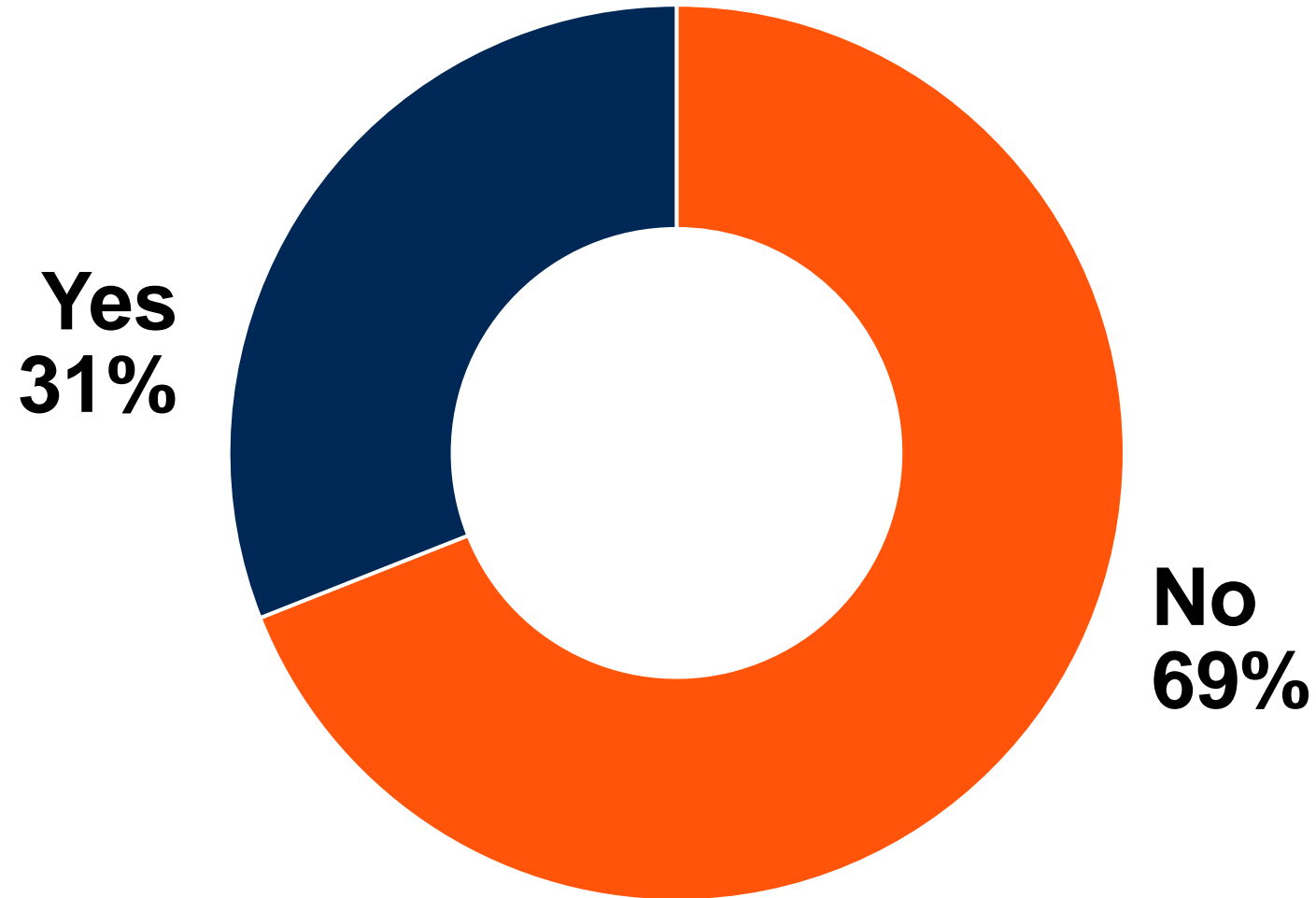
Goal of Effective Risk Management

Risk Exposure vs. Risk Appetite



Does the Business Use Risk Appetite?

Percentage of Heads of ERM Who Say the Risk Appetite is Regularly Consulted



What's Really Going On?

Reasons Why Business Leaders Fail to Act Within Risk Appetite

Mixed Messages

"I am unsure how I can follow leadership's guidance on risk appetite while also achieving the growth targets I've been given."



Silence

"I didn't realize my decision to invest in this new technology platform was outside our leadership's risk appetite."



Vagueness

"I know we have low tolerance for cyber security issues. If I use this particular vendor, does that align with the low tolerance?"



Key Issue Take-Away:

Whether a decision-maker is taking too much risk or too little, that is a problem.

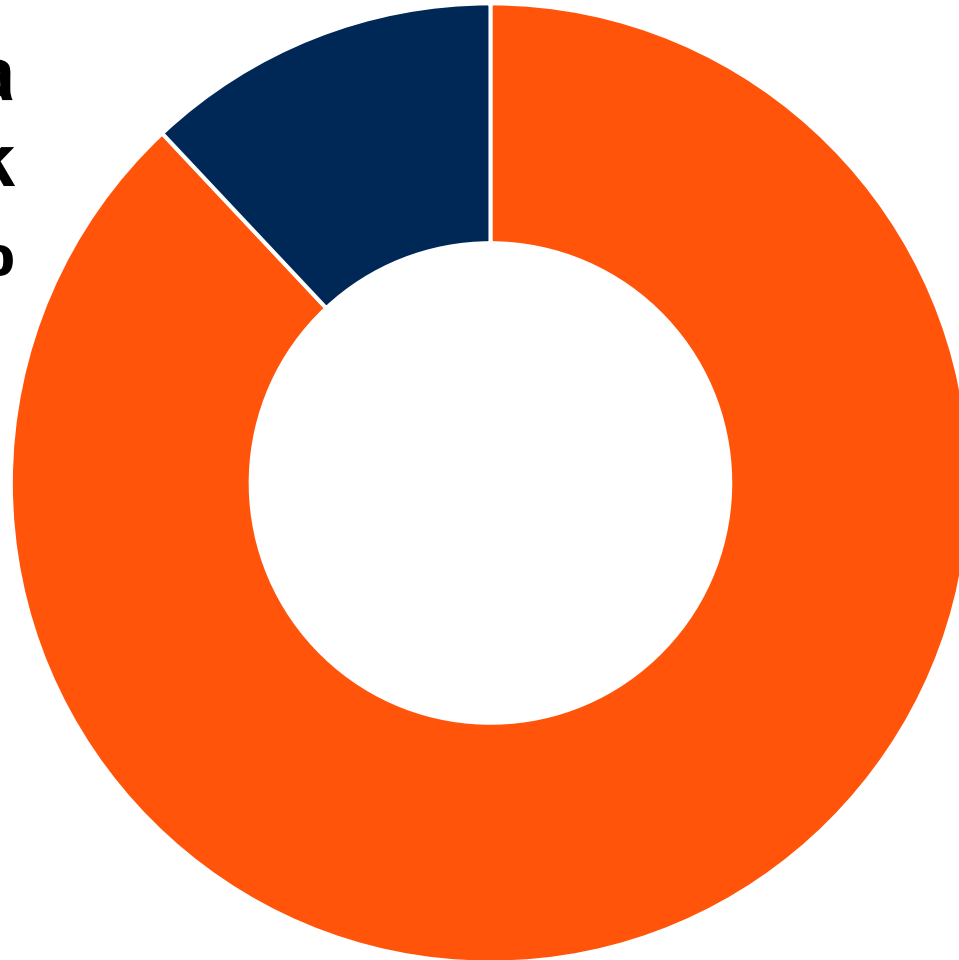
Key Issues

1. Risk appetite needs to be actionable
2. How to make risk appetite statements actionable
3. Ensure better buy-in to the risk appetite by the business

Boards see Cybersecurity as a Business Risk

How cybersecurity is viewed and handled by board directors

**Cyber is a
technology risk
12%**



**Cyber is a
business risk
88%**

Risk Appetite Ratings

The following ratings are used to articulate the level of risk appetite the Board is willing to accept in relation to each appetite category:

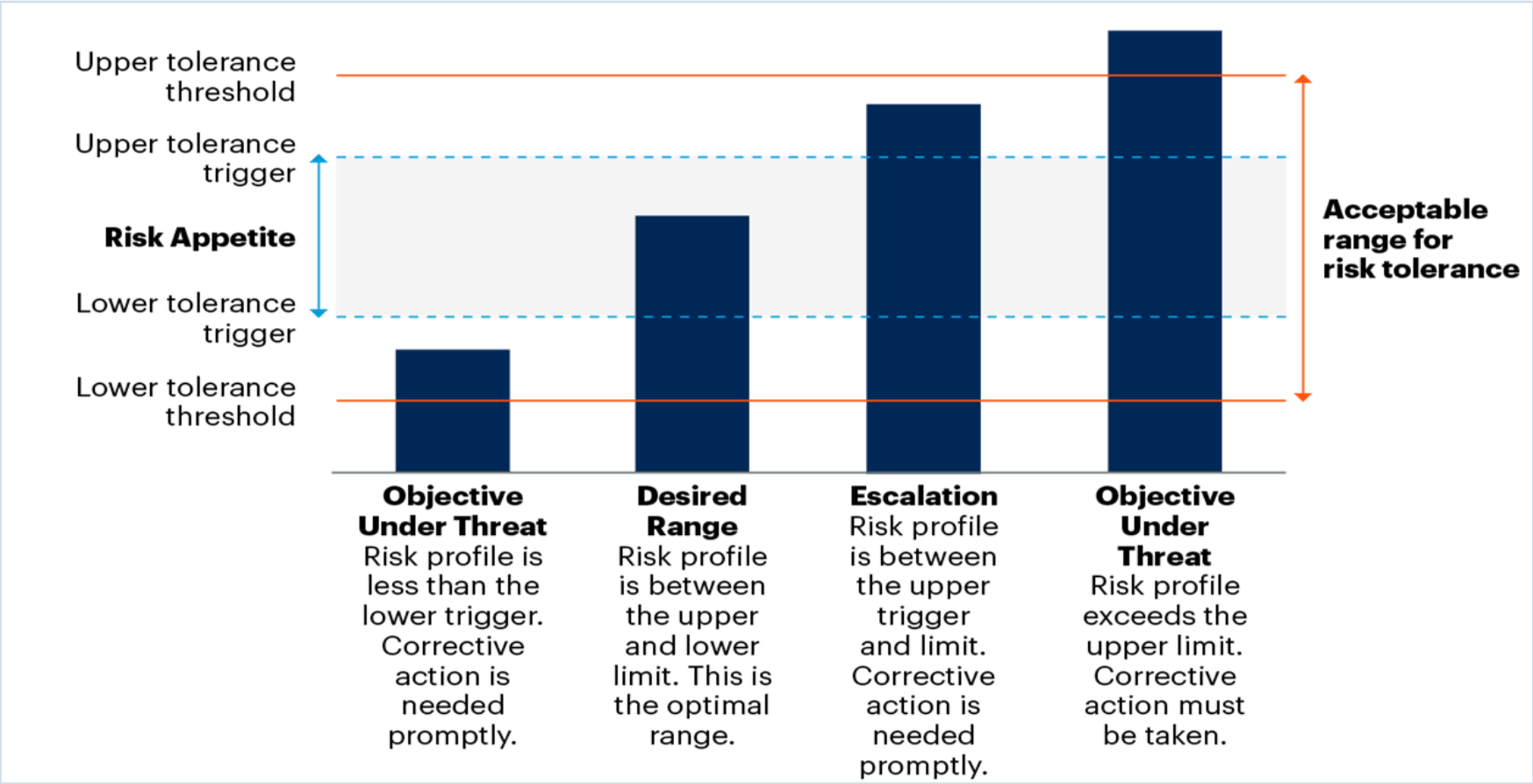
Illustrative

Rating	Averse	Minimalistic	Cautious	Flexible	Open
Risk-Taking Philosophy /Scale Definition	Not willing to accept risk (threats or opportunities)	Willing to accept a very limited amount of risk in situations where the benefits (opportunities) significantly outweigh the risk	Willing to accept some risk if heavily outweighed by benefits (opportunity)	Willing to accept risks equal to the possible benefits (opportunity) and will control the negative impact	Willing to accept a high level of risk in situations with significant opportunities

Key Risk Indicators (KRIs) and Tolerance

Key Risk Indicators (KRIs) and tolerances will be used to measure adherence to risk appetite. Risk tolerances are divided into the following categories:

Illustrative



Risk Appetite Statements

		Tolerance Indicators				
Appetite Category & Definition	Risk Appetite Statement	Metrics	Objective Under Threat	Desired Range	Escalation	Objective Under Threat
Talent Risk The risk that the organization's inability to recruit, engage and develop employees and leaders across all service lines to effectively and efficiently support organization goals and objectives.	We have a cautious appetite for talent management risk.					
	We strive to attract and retain top talent, recognizing that our industry requires us to seek top talent to be competitive. As such we will make every effort to develop staff skills, ensure completeive compensation and create an inclusive work culture.	Compensation deviation from industry standard	>+6%	+5% to -3%	-5 to -9%	<-10%
	We will make every effort to retain key talent. We will ensure successors are in place for all senior leaders.	Complaints Through the Employee Hotline	<4	5-12	13-25	>26
		Employee Turnover Rate	<6%	7-10%	11-20%	>21%
<div><div>AverseMinimalisticCautiousFlexibleOpen</div></div>						
[Category Name] <i>[Category definition]</i>	What = level of appetite	[Metric]				
	Why = reason why this level of appetite was chosen, considering corporate strategy, organisational objectives and values	[Metric]				
	How = details of what the organization is will to do to maintain this level of appetite	[Metric]				
	<div><div>AverseMinimalisticCautiousFlexibleOpen</div></div>					

Cybersecurity Sample Risk Appetite Statement

		Tolerance Indicators				
Appetite Category & Definition	Risk Appetite Statement	Metrics	Objective Under Threat	Desired Range	Escalation	Objective Under Threat
Cybersecurity Risk The risk to organizational operations (mission, functions, image, reputation), assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.	We have a <u>minimalistic</u> appetite for cybersecurity risk,	% of reported incidents involving PII	<1%	1% to 5%	7% to 9%	10%+
	Understanding we must use personally identifiable information (PII) about our customers and employees in the course of our business, we strive to create a robust and defensible cybersecurity program. We take a strategic, risk-based approach to cybersecurity to ensure appropriate and timely access to information while making sure we align to organizational goals in securing the organizations most critical information.	% of vulnerable information assets containing PII	<10%	10-20%	21-25%	>26%
		% of critical business processes with no tested disaster recovery plans	<10%	10-20%	21-25%	>26%
	<div><div>Averse</div><div>Minimalistic</div><div>Cautious</div><div>Flexible</div><div>Open</div></div> 					

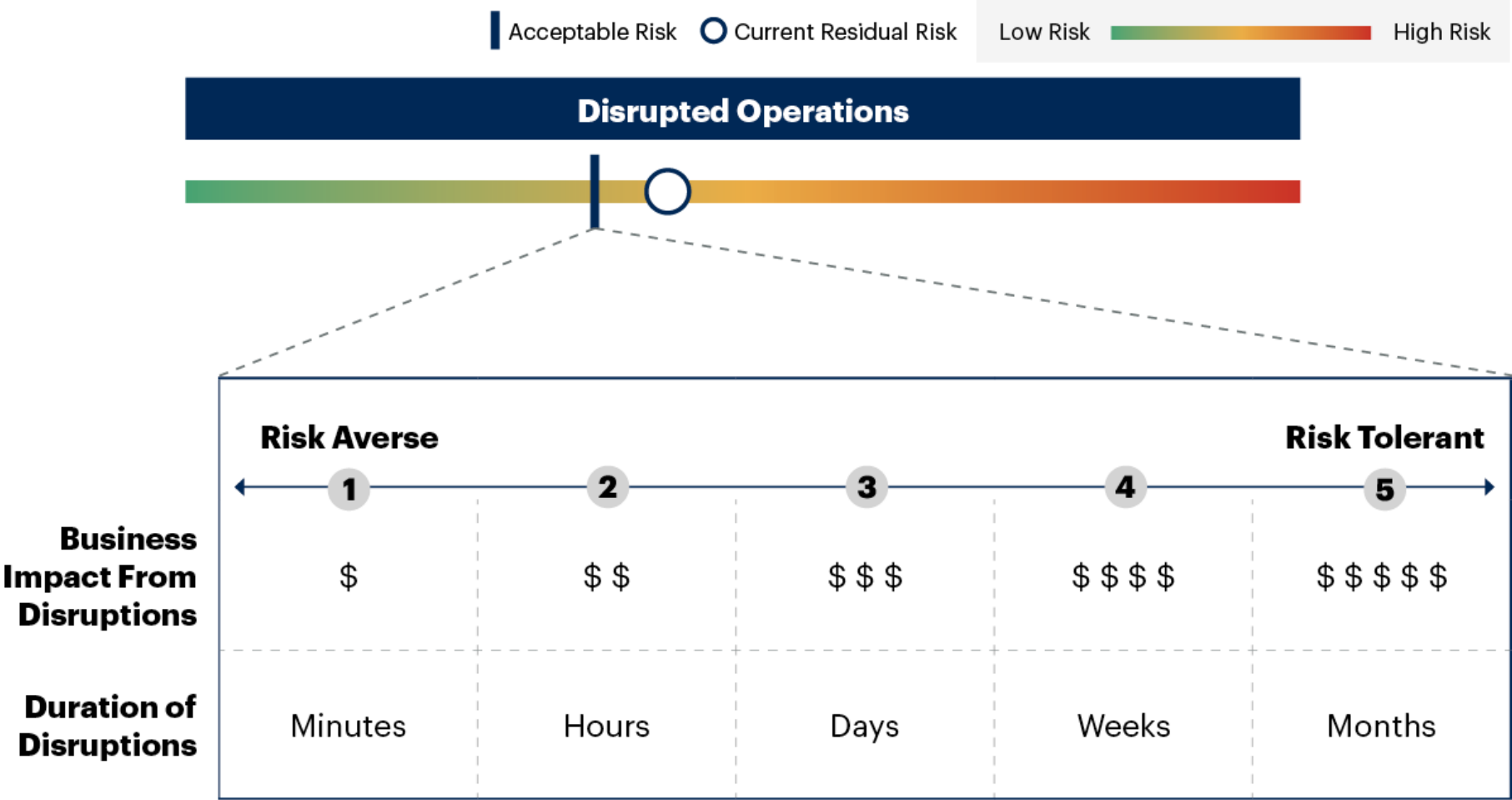
Key Issue Take-Away:

Actionable risk appetite statements include the **what**, **why**, and **how** as guidelines.

Key Issues

1. Risk appetite needs to be actionable
2. How to make risk appetite statements actionable
- 3. Ensure better buy-in to the risk appetite by the business**

Executives Need to Articulate Risk Tolerance



Risk Appetite Diagnostic

1. Gauge Risk Appetite Actionability

Do we have these?

- Actionable, common language to talk about risk appetite
- Clear guidance on how to make strategic tradeoffs and prioritize decisions

2. Assess Risk-Taking Behaviors

- Identify deviation from expected risk-taking behavior
- Conduct risk gap assessment workshops help find the gaps between target and exhibited risk appetite

1. Gauge Risk Appetite Actionability - Ask Three Questions

1. **Tolerance for Uncertainty:** How willing are you to accept uncertain outcomes?
2. **Choice:** When faced with multiple options, how willing are you to select an option that puts this objective at risk?
3. **Trade-Off:** How willing are you to trade-off this objective against achievement of other objectives?

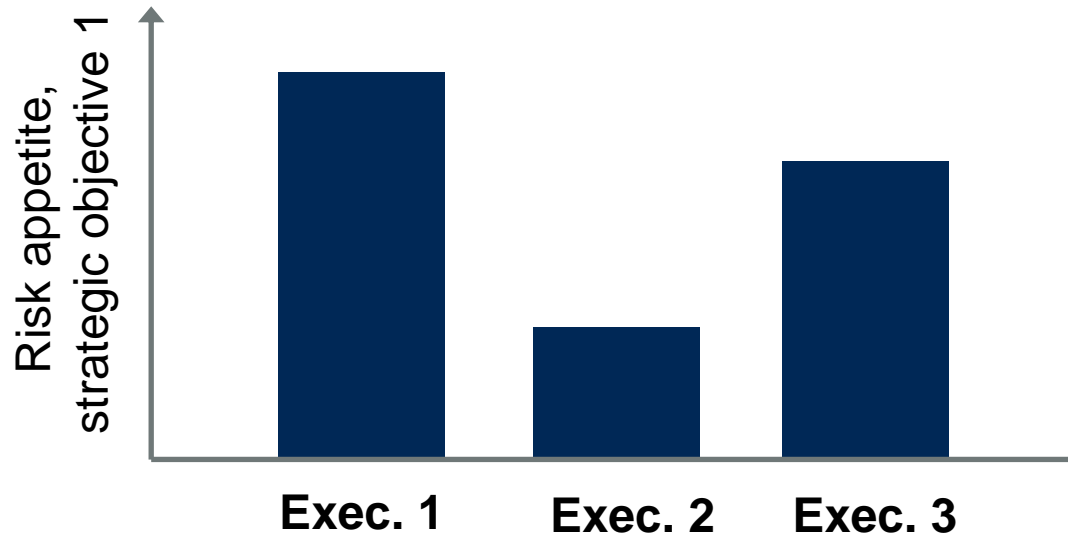
Qualitative Risk Appetite Rating Scale

Rating	Risk-taking philosophy	Tolerance for uncertainty How willing are you to accept uncertain outcomes?	Choice When faced with multiple options, how willing are you to selection an option that puts this objective at risk?	Trade-off How willing are you to trade-off this objective against achievement of other objectives?
5-Open	Will take justified risk	Fully anticipate	Will choose option with highest return; accept possibility of failure	Willing
4-Flexible	Will take strongly justified risks	Expect some	Will choose to put at risk but will manage the impact	Willing under certain conditions
3-Cautious	Preference for safe delivery	Limited	Will accept limited risk if heavily out-weighed by benefits	Prefer to avoid
2-Minimalist	Extremely conservative	Low	Will accept only if essential, and limited possibility/extent of failure	With extreme reluctance
1-Averse	“Sacred” Risk avoidance is a core objective	Extremely low	Will select the lowest risk option, always	Never

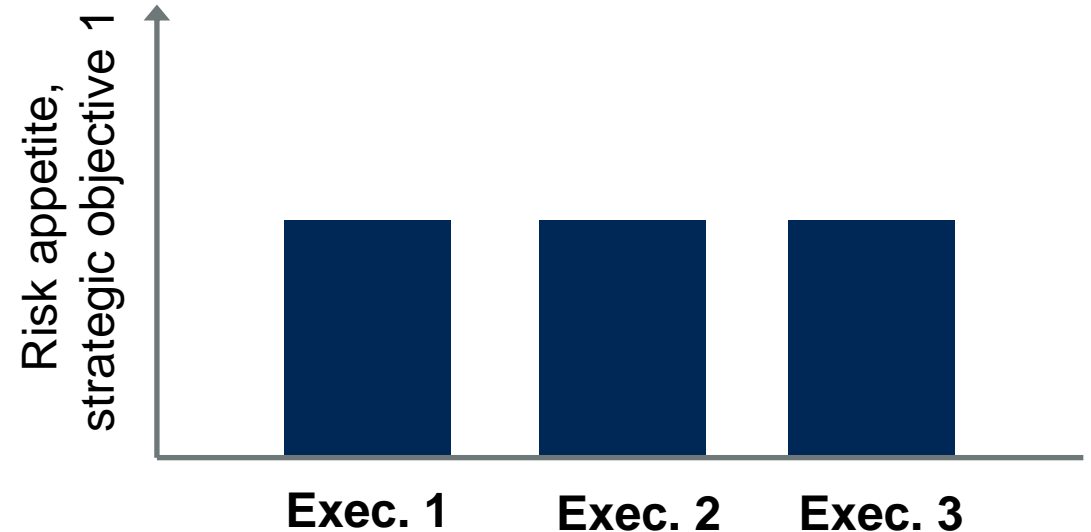
Refine Appetite in Risk Posture-Setting Workshops

Example approach

- Executives individually rate risk appetite for each strategic objective



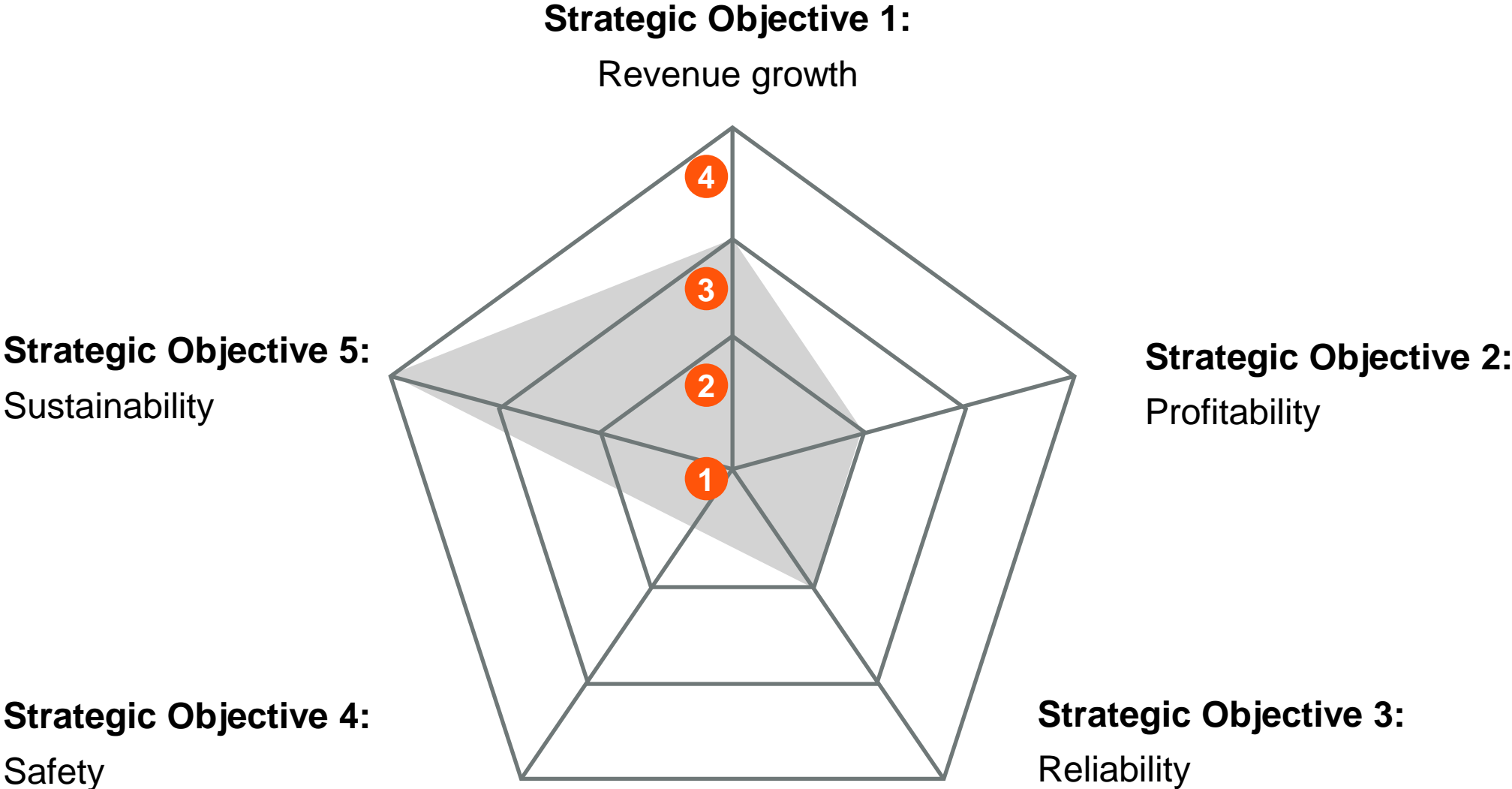
- Facilitator shares the mean
- Participants discuss their rationale, narrow their points of view



- Repeat if necessary

Plot Risk Appetite for Strategic Objectives

Example



2. Assess Risk-Taking Behaviors



Risk-Taking Behaviors Questionnaire (Example)

- 1. **What** risk appetite did executives exhibit in the way they set goals?
- 2. **How** were our strategic objectives communicated, resourced, and monitored?
- 3. **Which** objectives were put at risk (and **when**), citing the need to focus on another objective?

Results of risk behaviors questionnaire		
Strategic Objective	Target Risk Appetite	Exhibited Risk Appetite
Grow revenue	4-Flexible	4-Flexible
Increase profitability	3-Cautious	1-Averse
Become carbon neutral	4-Flexible	4-Flexible

Misaligned behaviors

Risk Appetite Gap Assessment (Example)

Strategic objective	Risk appetite	Actual/desired risk appetite assessment
Growth: Create three new growth platforms, each with \$300 million revenue potential	3-Cautious: Limited tolerance for uncertainty; prefer to avoid making trade-offs against achievement of other objectives.	<div>Actual Risk taking Desired Risk taking</div> 
Safety: have an injury-free workforce	1-Averse: Extremely low tolerance for uncertainty; never willing to accept trading-off this objective against achievement of other objectives.	<div>Actual/Desired Risk taking</div> 

Key Issue Take-Away:

Determine and communicate ideal risk-taking behaviors, and regularly assess deviation from these expectations.

Recommendations

- ④ Consult with a Gartner advisor on improving the actionability of your organization's risk appetite
- ④ Improve the actionability of your risk appetite statements – see Action Plan for CISOs two slides from now
- ④ Plan a Risk Appetite Workshop to help executives come to a consensus and learn from one another

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- 🔍 **Risk Appetite Formulation and Communication Template ([link](#))**
Alex Ossington
- 🔍 **Research Roundup for Risk Appetite and Risk Tolerance ([link](#))**
Enterprise Risk Management Research Team
- 🔍 **Six Steps to Manage Cybersecurity Risk Appetite Through Protection-Level Agreements ([link](#))**
Paul Proctor, Shruthi Shankel, Richard Addiscott et al.
- 🔍 **Match Higher Risk Appetite by Upgrading Internal Controls ([link](#))**
Julie Tani

Action Plan for CISOs

Monday Morning:

- *Estimate* the current actionability of your risk appetite statements
- *Discuss* the utility of making risk appetite more actionable with a senior leader

Next 90 Days:

- *Plan* a Risk Appetite Workshop per guidelines in this presentation
- *Conduct* a Risk Appetite Workshop with senior leaders

Next 12 Months:

- *Assess* executive behaviors and decisions for deviation from expected risk-taking
- *Revise* risk appetite statements to reflect changes in the risk environment



Thank You!