



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program

Toronto

May 28, 2026



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: AI as a Cross-Cutting Risk

Monica Kowal, Executive in Residence, GRI

May 28, 2026

Is AI creating new risks that belong somewhere in your existing framework, or is it changing the conditions under which all enterprise risk must be governed?

Which describe your organization's current approach to AI risk?

- We treat AI primarily as a model risk or technology risk issue, managed within those existing functions
- We have created a standalone AI risk category that sits alongside our other risk categories in the ERM framework
- AI risk is discussed across multiple committees, but we do not yet have a unified view of whether our ERM architecture is fit for purpose
- We are actively redesigning our ERM architecture to govern AI at scale

WhitePine Financial Holdings | A Case Illustration

The Credit Adjudication Platform | Machine Learning

- What risk categories were active in that scenario?
- Where was the governance weakness? Was it model risk? Compliance? Business leadership?
- How can a model be performing correctly on every metric that model risk was tracking and still produce outcomes the bank did not intend?

The Other Two Scenarios

The Call Centre Assistant | Generative AI

What does that difference mean for how you would approach governing each?

The Cash Management Tool | Agentic AI

What would have needed to be in place for any one of those override attempts to have been effective?

FIFAI II: The AGILE Framework



AWARENESS: Stay ahead of AI-driven risks by understanding how technologies reshape the risk landscape through organizational enhancements such as AI oversight, board engagement, and expanded monitoring and stress testing scenarios.



GUARDRAILS: Make best practice regular practice with strong controls, data-integrity standards, human oversight for high-impact decisions, transparency and appropriate consumer outcomes, and rigorous third-party oversight.



INNOVATION: Adopt an AI growth mindset that treats AI as a driver of competitiveness and enhances consumer financial well-being and protection, supported by bold investments in talent, modern infrastructure, and responsible innovation.



LEARNING: Build AI skills at every organizational level, including employees and management, through continuous training and collaborative initiatives, while also empowering consumers with AI literacy to help them protect themselves and make informed choices.



ECOSYSTEM RESILIENCY: Fortify system-wide defences through improved third-party oversight, regulatory clarity, enhanced digital identity security, expanded real-time threat sharing, and upgraded incident-response frameworks.

Is AI creating new risks that belong somewhere in your existing framework, or is it changing the conditions under which all enterprise risk must be governed?

- AI creates new conditions that challenge how ERM is architected
- Most governance frameworks carry a prevention assumption worth examining



Breakout Q1

Credit adjudication: Monitoring and detection

Model risk confirmed that performance metrics remained within approved tolerances throughout.

Yet the model was declining applications and overpricing new facilities beyond what WhitePine's own credit policies would support.

- What monitoring of model outcomes rather than model performance metrics would have detected this earlier?
- At WhitePine, who might be best placed to take responsibility for that monitoring, and what expertise would they have needed to assess what they were seeing in real time?
- What outcomes, behaviours, or customer impacts should have been treated as risk indicators even though traditional model metrics remained stable?

Breakout Q2

Credit adjudication: Remediation

WhitePine now has a backlog of potentially affected lending decisions: wrongful declines and overpriced new originations.

- What would a credible remediation program require in terms of reviewer capacity, access to application files and model decision records, and credit judgment exercised independently of the model under review?
- What does the FCAC 56-day complaint resolution requirement mean for how quickly that capacity must be mobilized, and what would WhitePine, in hindsight, have been well advised to build into the model before deployment to facilitate complaint resolution?

Breakout Q3

Call centre: Detection and remediation

The generative AI assistant was operating as designed and yet customers received subtly incorrect information about their loan terms and entitlements. No threshold was breached and no metric flagged a problem. Unlike the credit adjudication scenario, there is no defined backlog of identifiable decisions to review.

- What does this reveal about the limits of traditional monitoring for this type of AI system, and what would identifying and remediating affected customers require?
- What design-stage decisions would have made it possible to detect this problem earlier and identify which customers were affected?
- What level of logging, retention, and interaction traceability would have been necessary to investigate the issue effectively after the fact?

Breakout Q4

Cash management: Governance of agentic systems

The agentic cash management system operated within its pre-approved parameters throughout the market disruption. Yet treasury staff could not determine what it was doing or why, override attempts created conflicting instructions, and escalation to senior leadership became congested.

- What does this reveal about the limits of parameter-setting as a governance mechanism for agentic AI systems?
- What authorization architecture and human oversight design would WhitePine need before deploying this kind of system at operational scale?

Breakout Q5

Cross-cutting: Accountability

Across all three events, each function operated within its defined lane and WhitePine was still blindsided.

Consider both the first line business functions that deployed and operated these systems and the second line oversight functions responsible for the risk framework.

- Where should accountability for end-to-end AI system outcomes sit in the first line, and what coordination and integration role should the second line play to ensure that what each function sees is assembled into a coherent picture?

Breakout Q6

Cross-cutting: Governance designed to cope with problems in production

In all three events, problems reached customers and regulators before WhitePine's internal governance detected them as enterprise risk events. WhitePine's governance architecture appears to have been designed around the assumption that controls would prevent problems from reaching production.

- What is different about governance architecture designed to cope with AI-related problems in production from the architecture WhitePine had in place, and what would need to change?
-

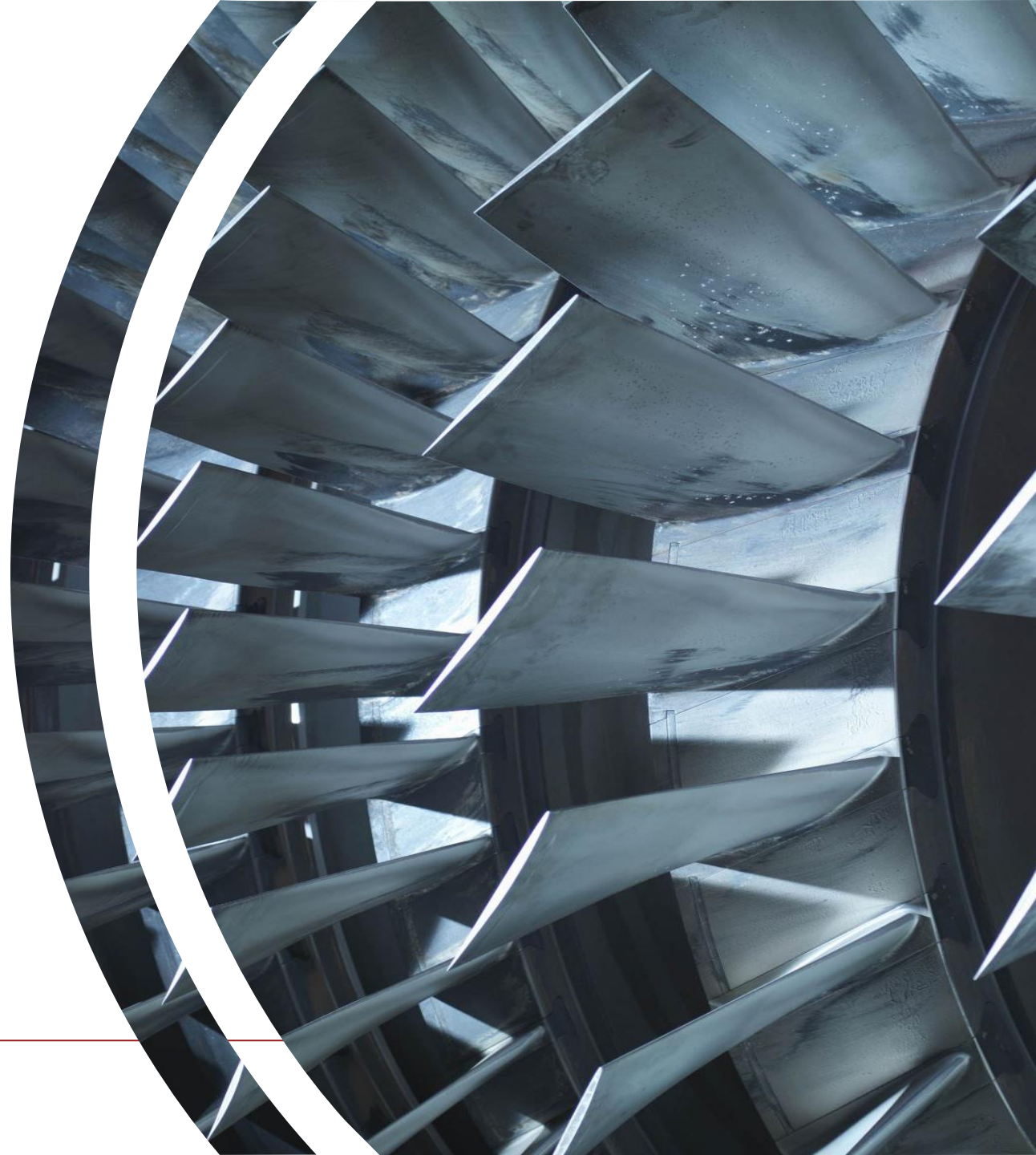
The Accountability Architecture

- **First line:** named individual accountability for AI system outcomes
- **Second line:** coordination and integration of oversight across functions



Governance Embedded in Design

- Evergreen control frameworks
- Circuit breakers and kill switches
- Bounded autonomy
- Deterministic guardrails
- Intent and execution observability
- Reversibility requirements



Governance Embedded in Design

Which assumptions in current ERM architecture were designed for a stable technology are now under stress from AI?

"The financial institutions and countries that move decisively will establish the standards and capabilities that define the next decade of financial services. Those that hesitate will find themselves following."

Strategic Actions for AI-Enabled Financial System Resilience, GRI, May 2026

Break



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: Operational Resilience - A Strategic Imperative

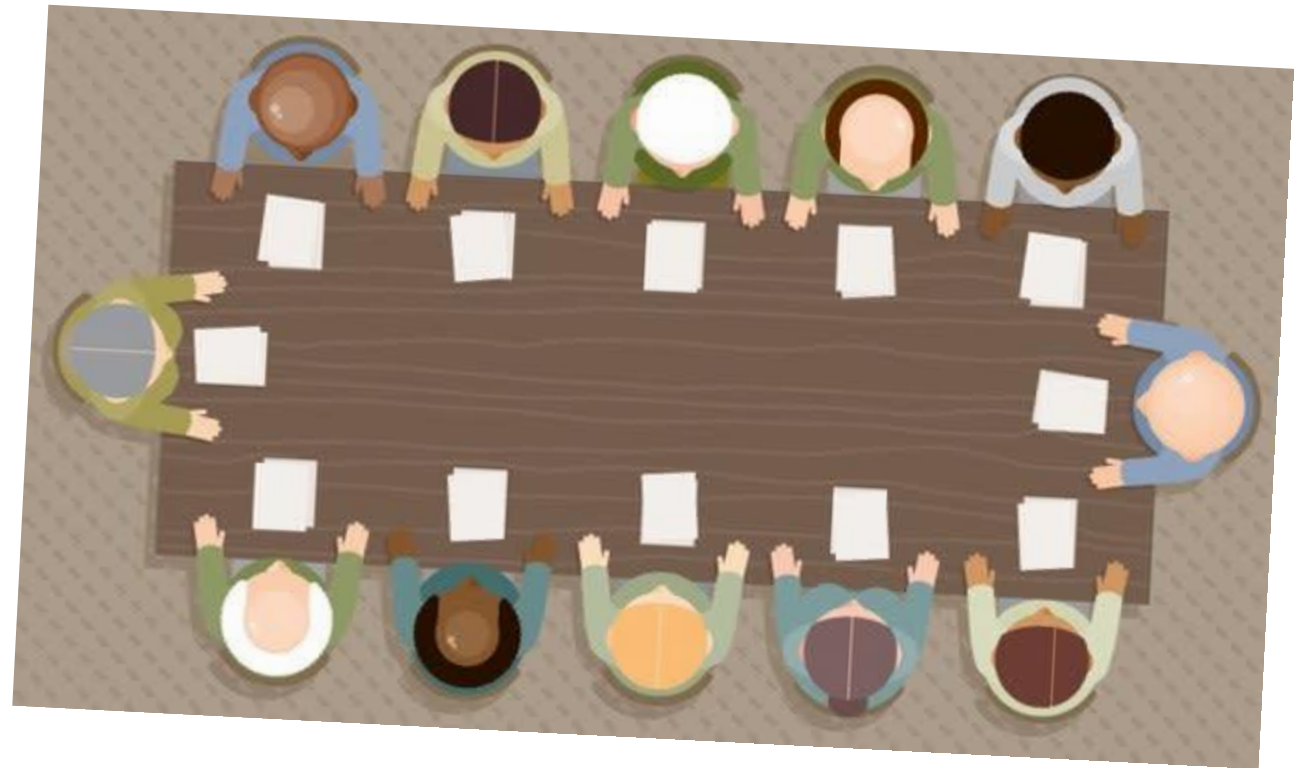
Gerard McDonald, Executive Consultant, GRI

May 28, 2026

Agenda

1. Introduction
2. Operational Resilience and its importance
3. Managing the impact of a significant Operational Resilience event - COVID pandemic
4. Developing Operational Resilience in your organization
5. Challenges to building Operational Resilience
6. Managing Operational Resilience
7. Closing

Is “Operational Resilience” on your Agenda?



What is Operational Resilience

“Operational resilience is about the agility to move and operate in different ways when circumstances change.” – McKinsey (2025)

- Operational resilience is the ability to deliver critical operations through disruption, short and long term
- An organization must identify, protect and recover from threats and potential failures
- It must also learn, respond and adapt to disruptive events and changes, capturing potential opportunities

“Robust operational risk management and resilience enhance the ability to prevent, detect, respond to, and recover from adverse events, while continuing to deliver critical operations.”

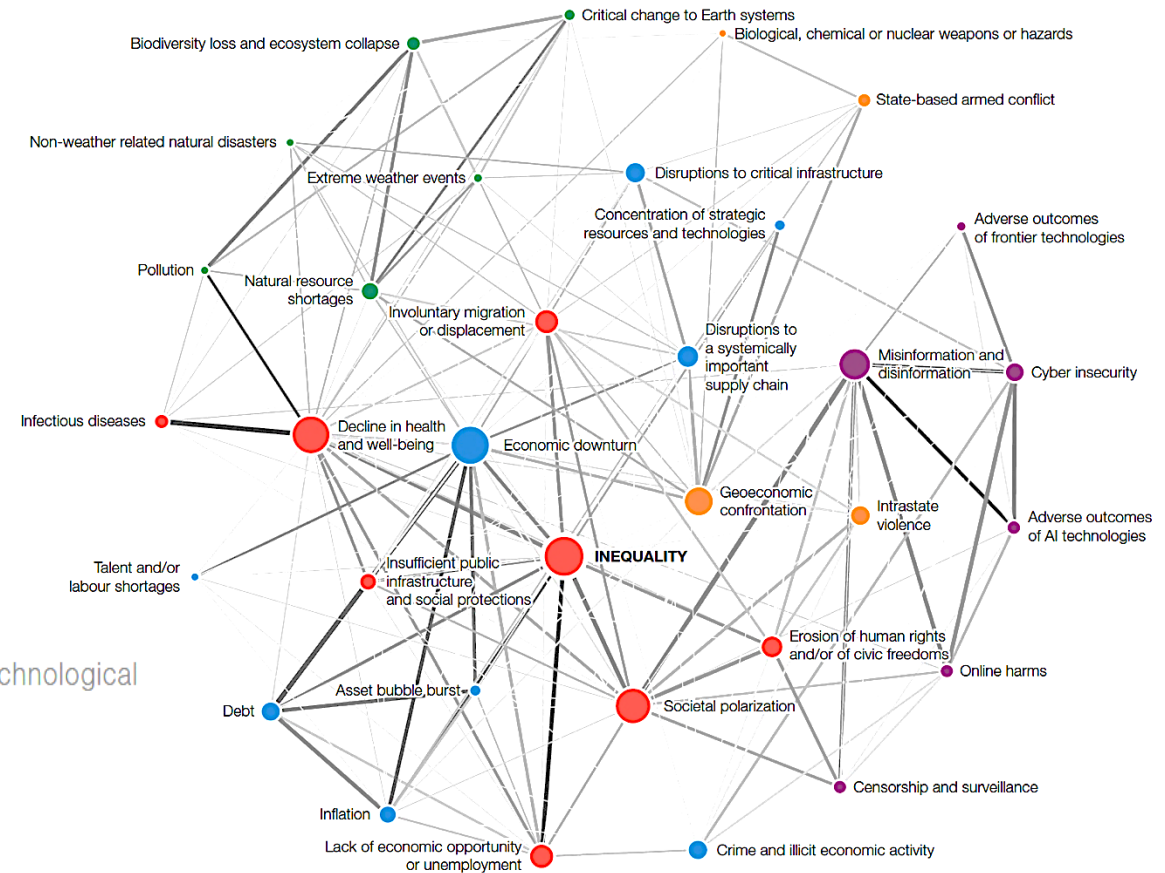
– Office of the Superintendent of Financial Institutions,
Guideline E-21 (2024)

“Operational resilience is defined as initiatives that expand business continuity management programs to focus on the impacts, connected risk appetite and tolerance levels for disruption of product or service delivery to internal and external stakeholders (such as employees, customers, citizens and partners).”

– Gartner (2025)

Why is Operational Resilience so important now?

“The 21st edition of the Global Risks Report 2026 reveals an increasingly fractured global landscape, where escalating geopolitical, environmental, societal and technological challenges threaten stability and progress.”



Risk categories: Economic (blue), Environmental (green), Geopolitical (orange), Societal (red), Technological (purple)

Nodes: Risk influence (High, Medium, Low)
 Edges: Relative influence (High, Medium, Low)

Source: World Economic Forum Global Risks Perception Survey 2025-2026

COVID pandemic: Importance and challenges of Operational Resilience

COVID showed “that government and public service organizations must be able to adapt and respond to change quickly, to maintain critical operations and services—as well as provide extraordinary supports and services to people, businesses, and communities.” – Deloitte (2022)



COVID required transformational changes to be made almost overnight and with significant restrictions in operating conditions

What are the key elements of a successful Business Continuity (BC) Program?

- Effectively engage and empower your team to ensure their commitment and readiness in delivering BC initiatives
- Establish streamlined processes that facilitate efficient communication and delivery of BC plans and initiatives
- Explore the importance of leveraging technology to enhance communication and collaboration

Business Continuity Planning (BCP) is an important part of Operational Resilience, but Operational Resilience goes far beyond BCP

What are the key elements of Operational Resilience?



- Identify key services
- Set an impact tolerance for disruption for each important service
- Ensure delivery of important services within impact tolerances during severe but plausible scenarios

Operational Resilience should also be seen as an opportunity. Developing Operational Resilience can identify ideas to increase effectiveness and efficiency.

How do you go about developing Operational Resilience?



Have a clear understanding of your most important services

Example of customer support to global merchants



Create a comprehensive understanding and mapping of the systems and processes that support these services (including 3rd Parties)

Need for staff to work alternative shifts



Define impact tolerances that drive the levels of resilience required for a service

Fast response required for international clients



Test plans that would enable firms to continue or resume services when disruptions occur

Implement remote and hybrid arrangements



Set up effective internal and external communications to keep stakeholders informed and maintain confidence in the organization and the services it provides

Client service seamless and happier workforce

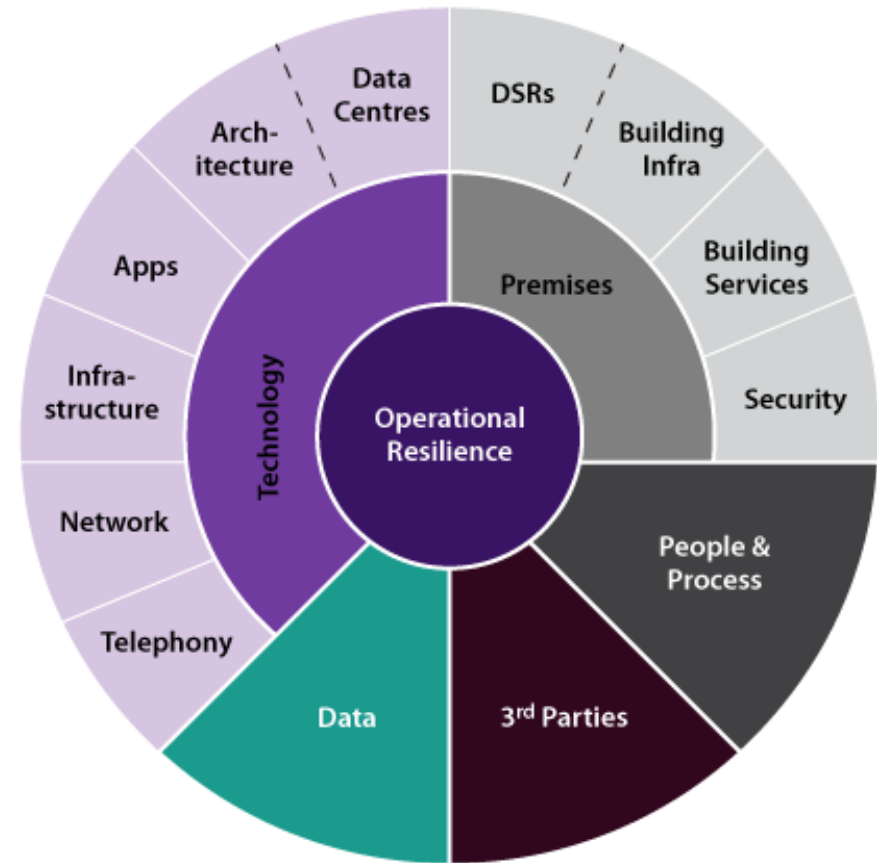


Operational Resilience is a key issue on which senior management should focus; whilst reducing risk, organizations should assume services will be disrupted and prepare accordingly

Agility critical to helping Shopify manage COVID

Protecting the assets that deliver services

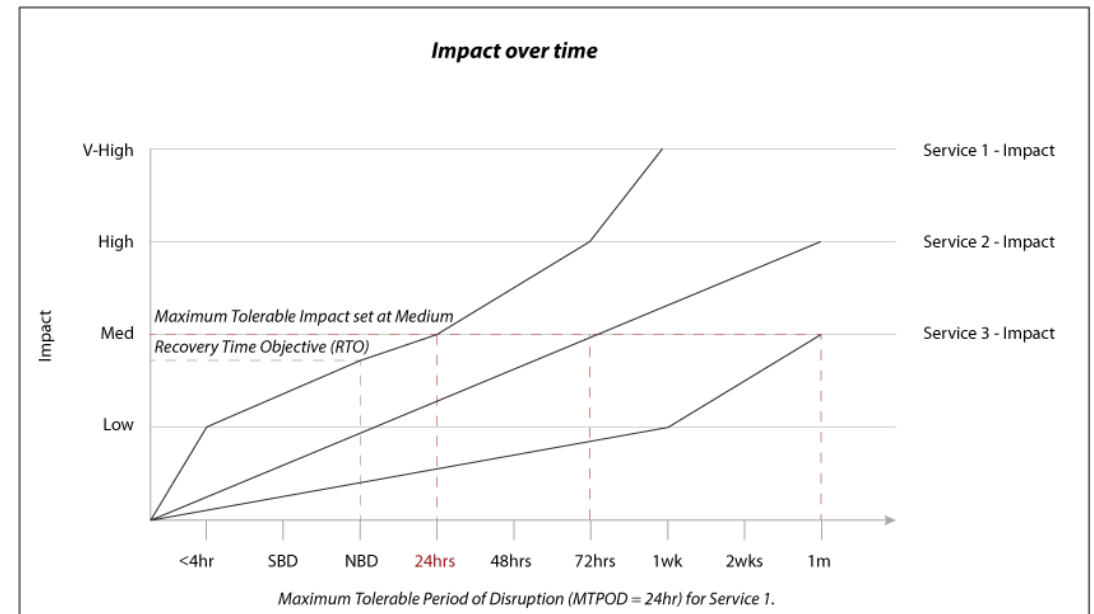
- Resilient organizations have a clear understanding of which assets underpin their services
- And protect those assets to a level that limits any impact to the tolerance agreed.



You must define how much disruption is acceptable for your key services

(e.g., how many hours can systems be down)

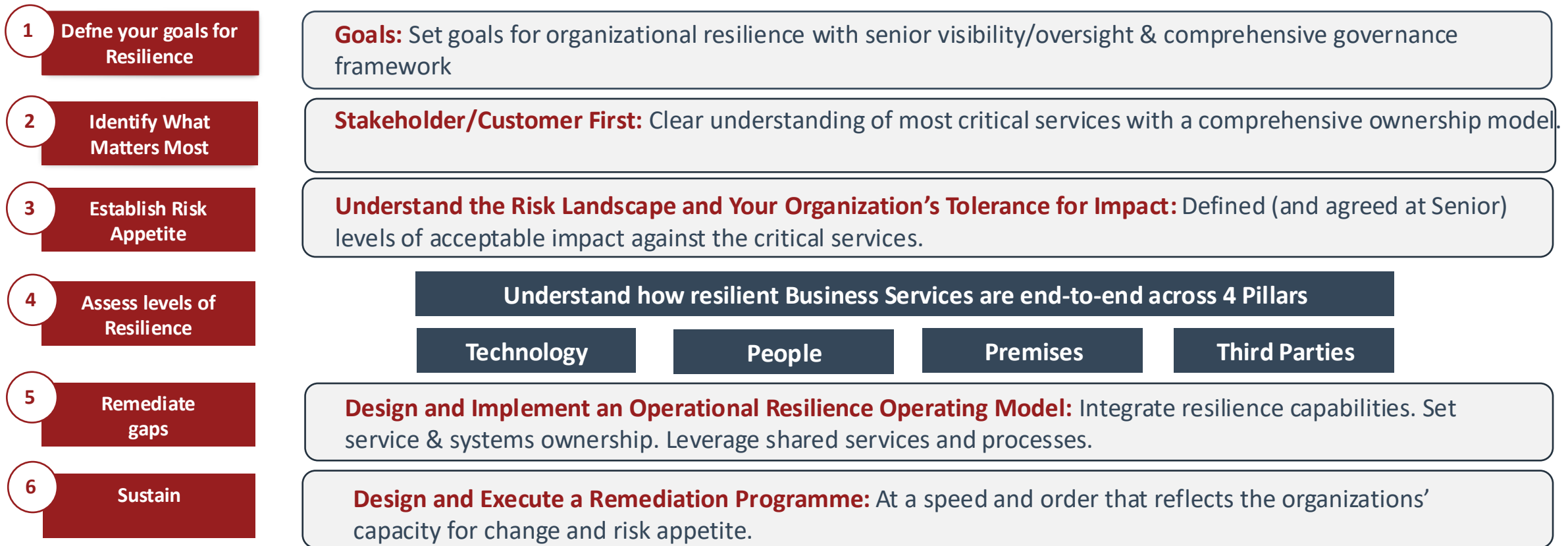
- You must have absolute clarity regarding how much impact you are willing to tolerate for each service, e.g. to customers, reputation, regulatory obligations.
- Where an impact hits designated tolerances, this will identify timeframes and priorities that will drive the levels of protection, monitoring and recovery a service has.



Risk Appetite is a critical part of Operational Resilience

E.g.: Approach to Operational Resilience

This approach is designed to create a top-down approach, understood and overseen by senior management, but requiring deep involvement from all levels

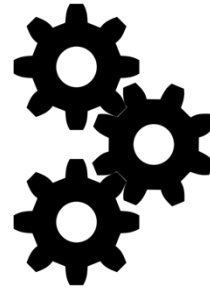


Challenges to building resilience



Innovation & change

Tolerance to downtime has reduced as services have become more digital



Keeping pace

Large volumes of change pose a risk to service continuity



Challenging environment

Outsourcing has lower cost but increases organizational complexity

An increasingly complex world has increased the need for Operational Resilience

Technological Advances, such as AI

- AI present opportunities in areas such as improved customer services, automation of routine work and predictive healthcare
- AI also presents challenges such as accelerating cyber attacks, mis/disinformation and potentially disruptive workforce changes

Geopolitical Developments

- Interconnection can lead to simultaneous interaction of multiple, diverse outcomes
- Changes can lead to new and positive political and trading relationship, but also increasing trade frictions and economic downturns

Given elevated uncertainty, strategic actions are needed to respond and build resilience

What can you do to support Operational Resilience in your organization?

- Proactively identify and mitigate risks and surface and capture opportunities
- Build strong relationships with third parties
- Advocate for continuous improvement in processes and systems
- Develop effective communication plans
- Deliver actionable reporting to stakeholders

Thank You





**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: **Risk Actions**

Michael Stramaglia

Toronto

May 28, 2026

Learning Objectives

- Understand the relationship between Inherent Risk, Residual Risk, and Risk Actions and how these elements are informed by Risk Appetite and Assessment
- Develop appreciation of potential “unintended consequences” and how these might undermine the effectiveness of management’s Risk Actions
- Gain appreciation of Risk Trade-Offs and Contagion Risk and how these should help to shape management’s Risk Actions

Inherent and Residual Risk

Inherent Risk (“gross” risk)

Risk of loss in the absence of any applicable risk actions

Residual Risk (“net” risk)

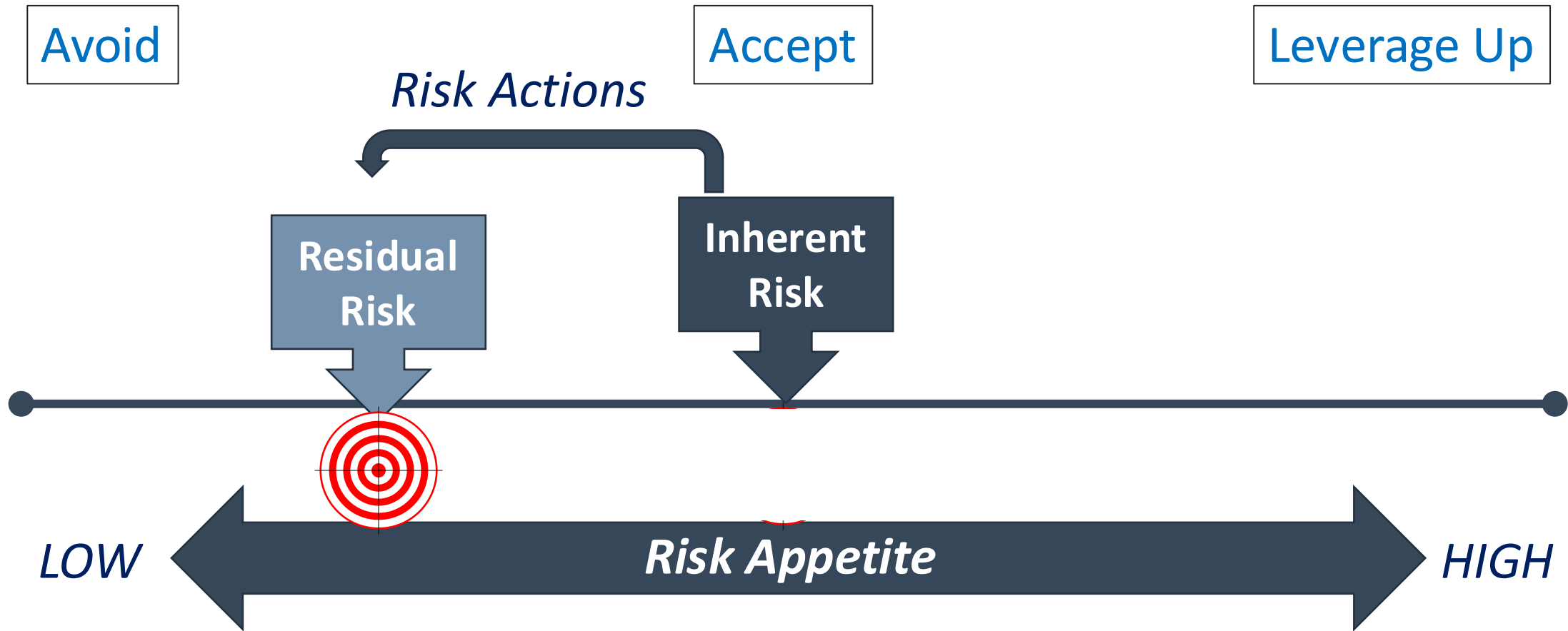
The risk that remains after taking into account applicable risk actions

Risk Actions

The set of strategies and tactics that management applies to transform inherent risks into a more desirable residual risk profile

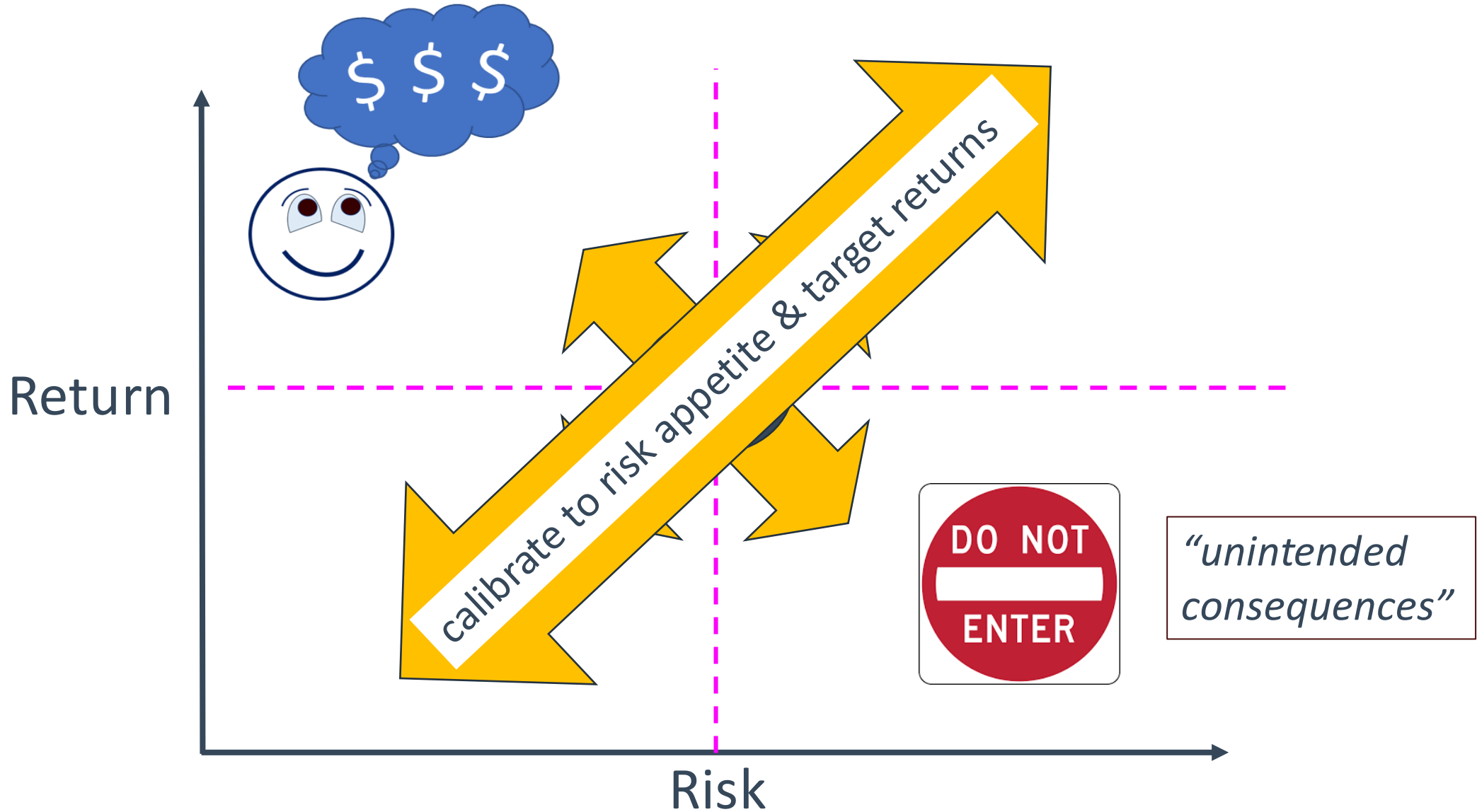
$$\text{Residual Risk} = \text{Inherent Risk} - \text{Net Impact of Risk Actions}$$

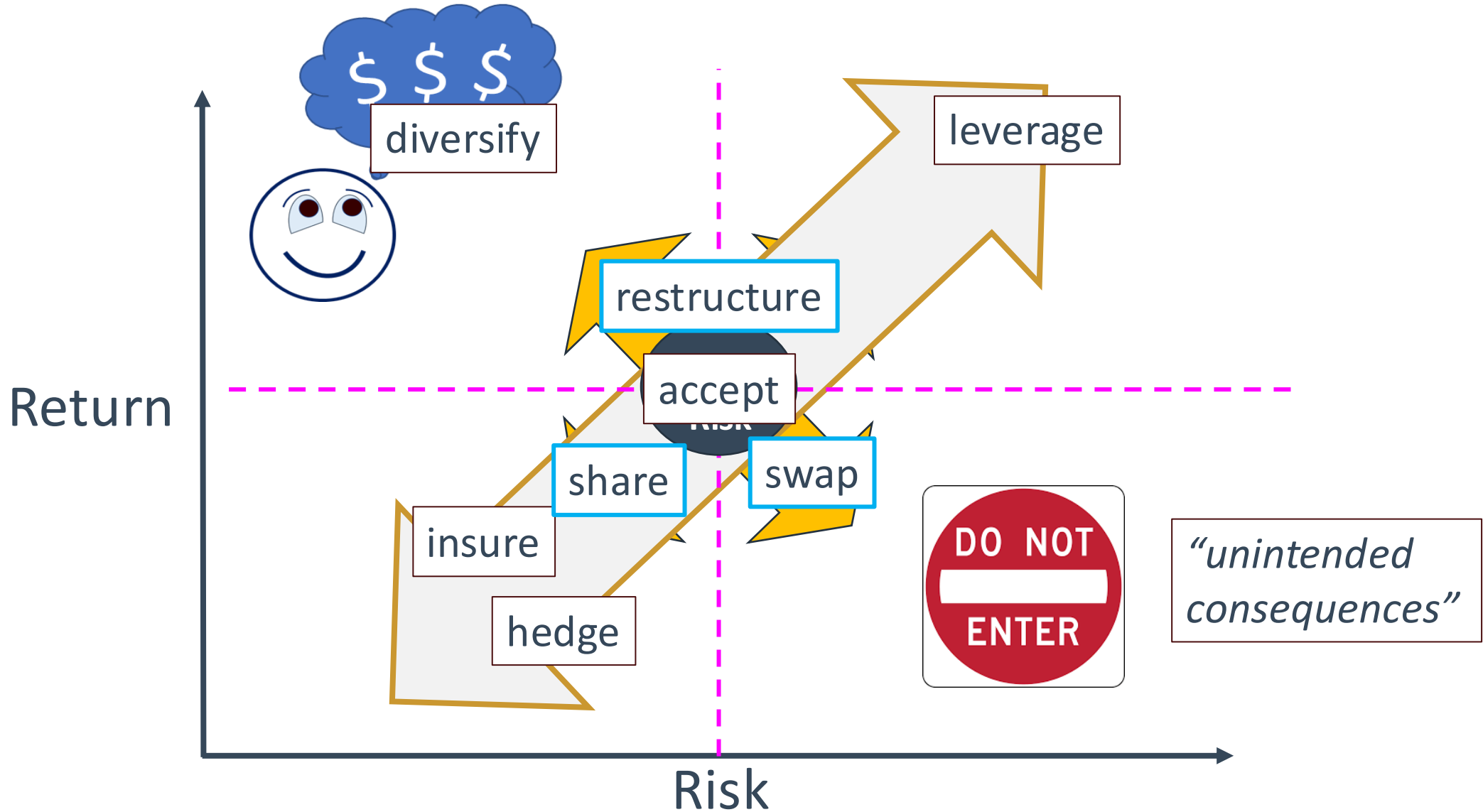




$$\text{Residual Risk} = \text{Inherent Risk} - \text{Net Impact of Risk Actions}$$







$$\text{Residual Risk} = \text{Inherent Risk} - \text{Net Impact of Risk Actions}$$

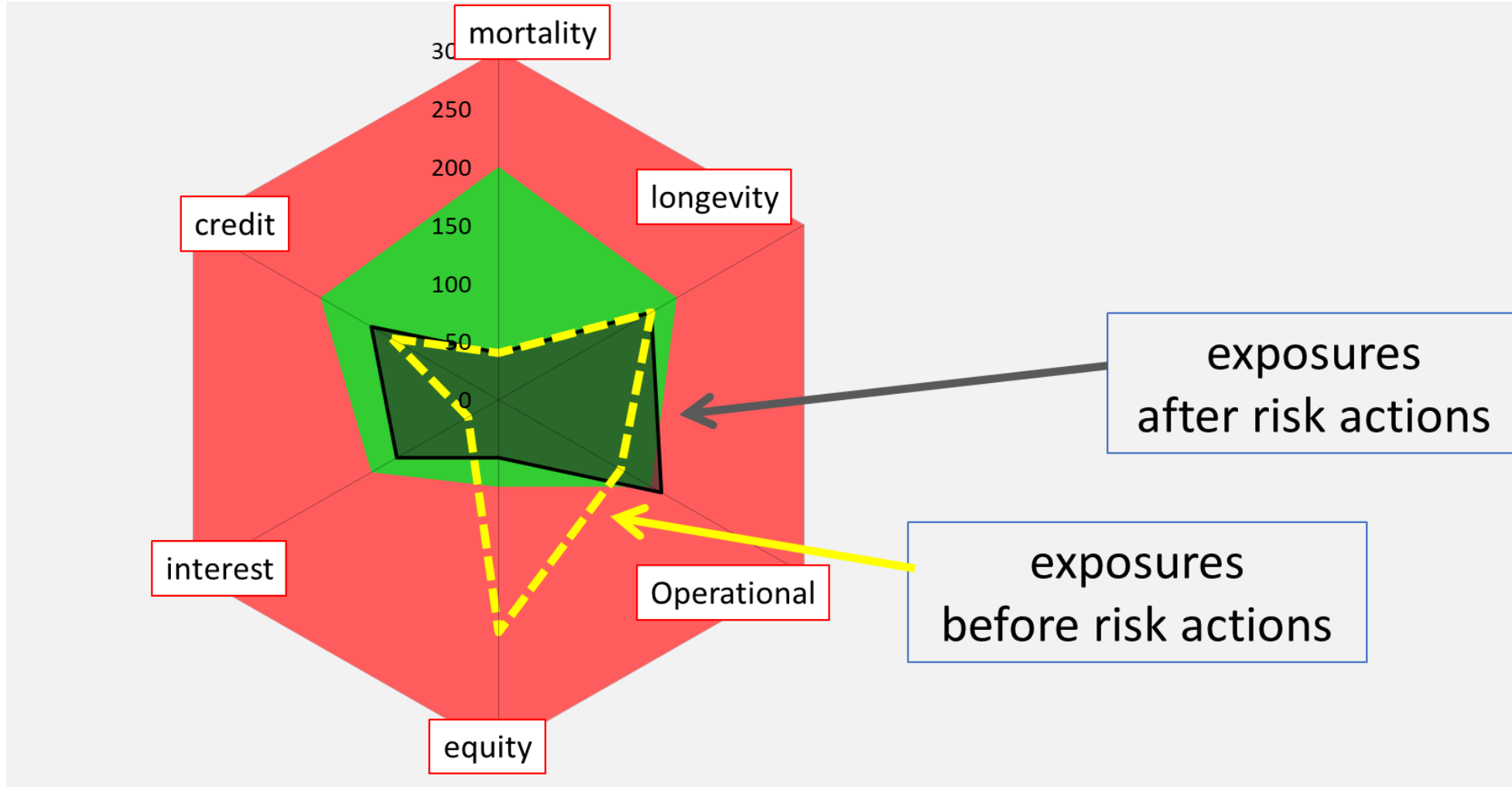


Which would you prefer?

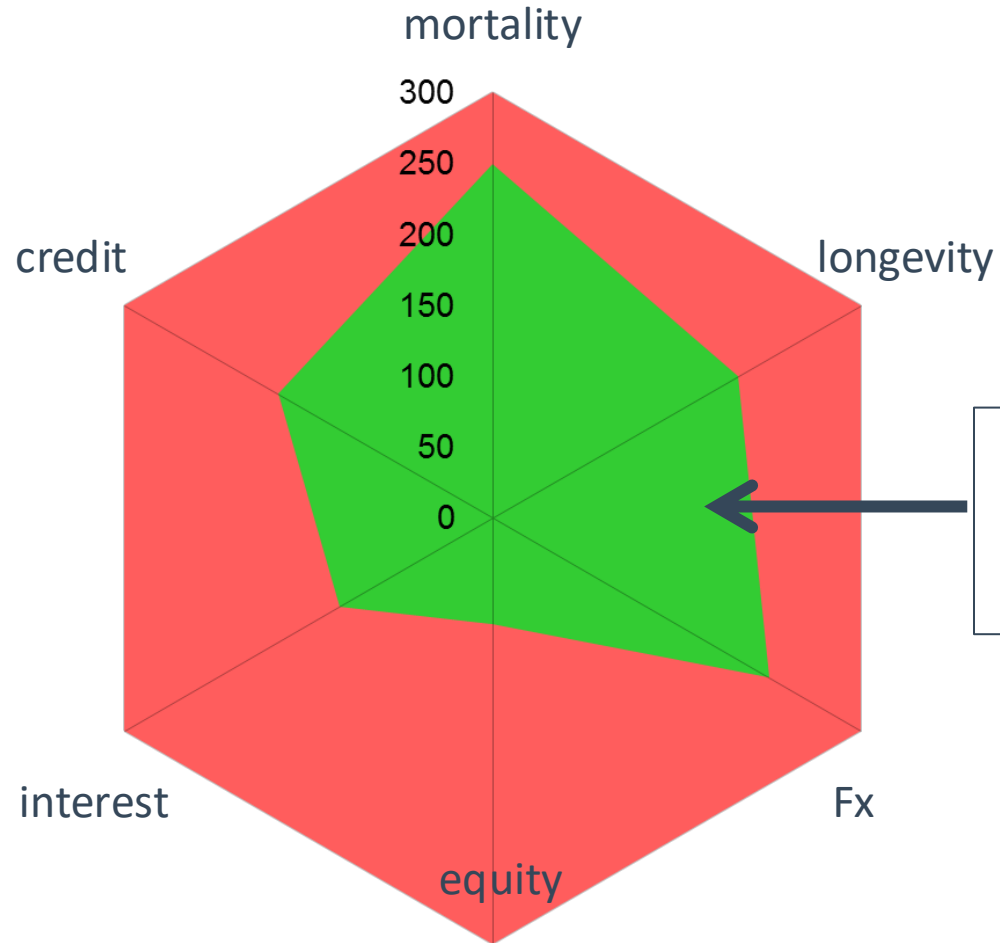
	Opportunity A	Opportunity B
Expected Return (RoE)	14%	13%
Residual Risk*	10	12

* Based on applicable VaR measure

Inherent and Residual Risk Visibility

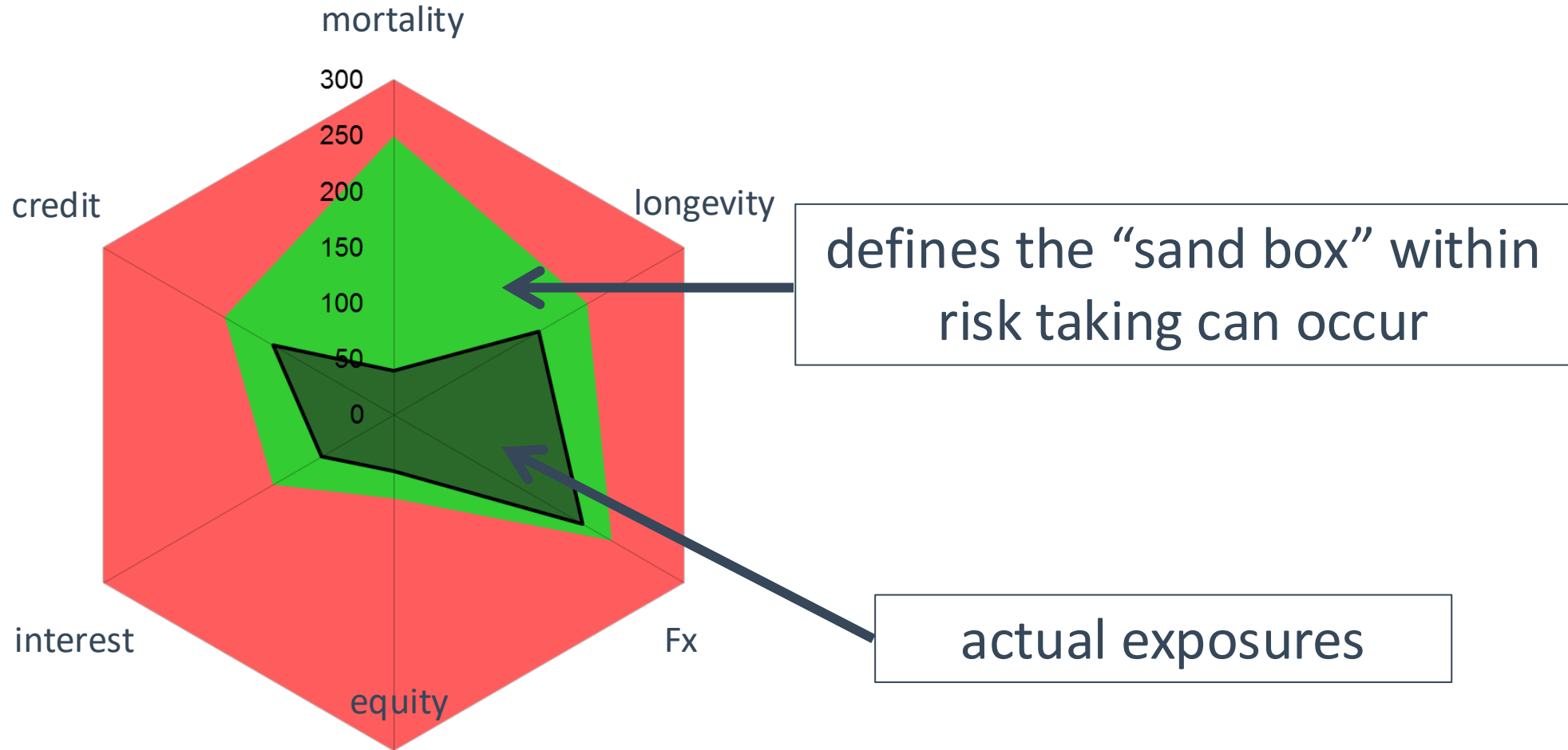


Risk Appetite Design

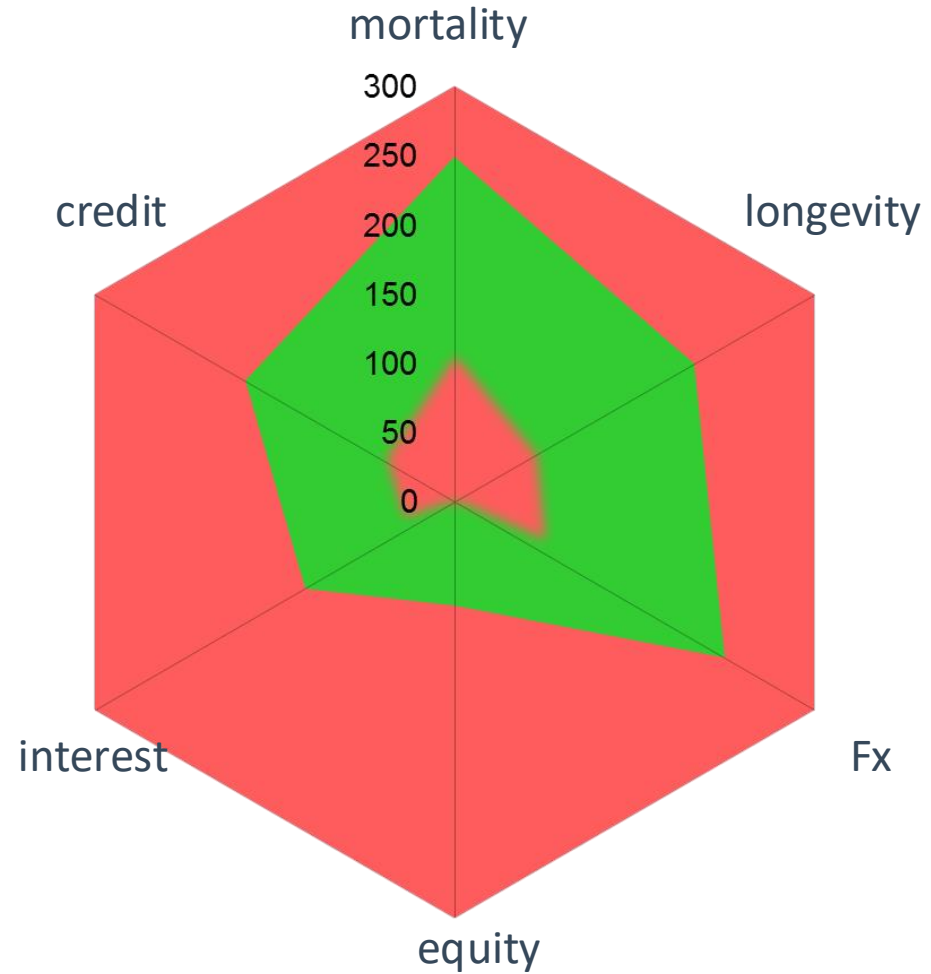
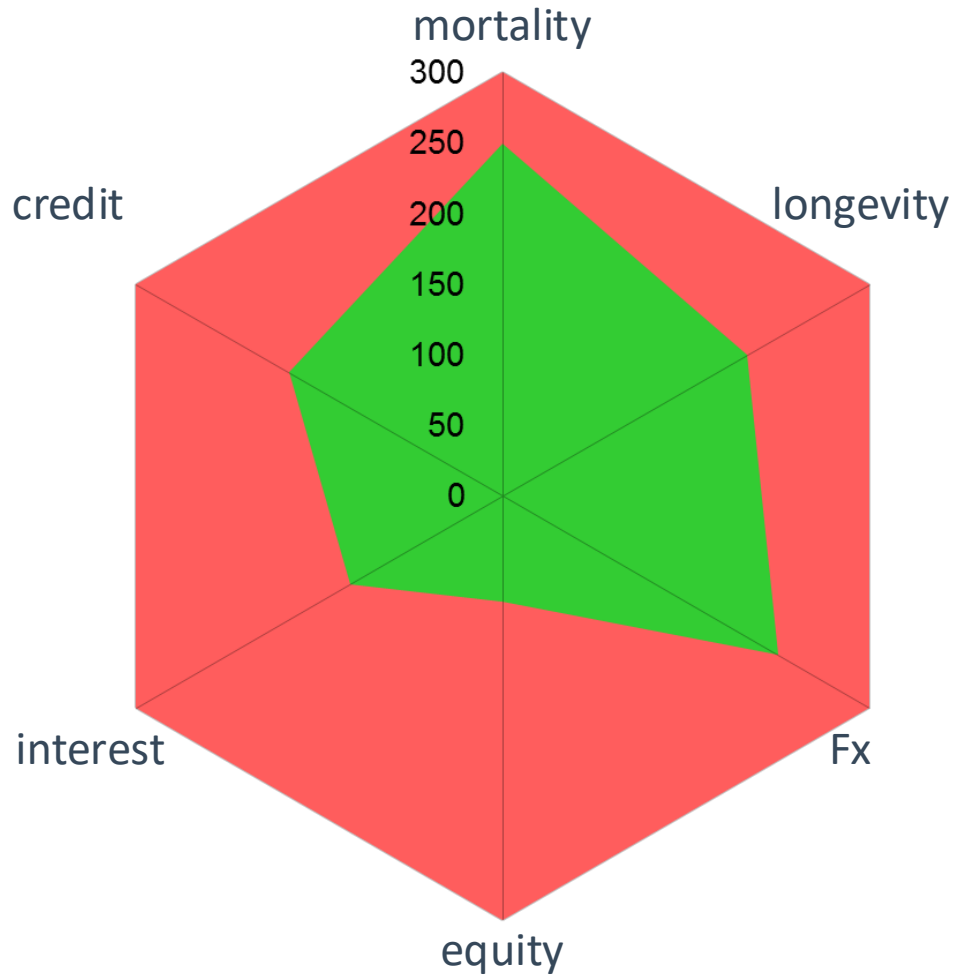


defines the “sand box” within risk taking can occur

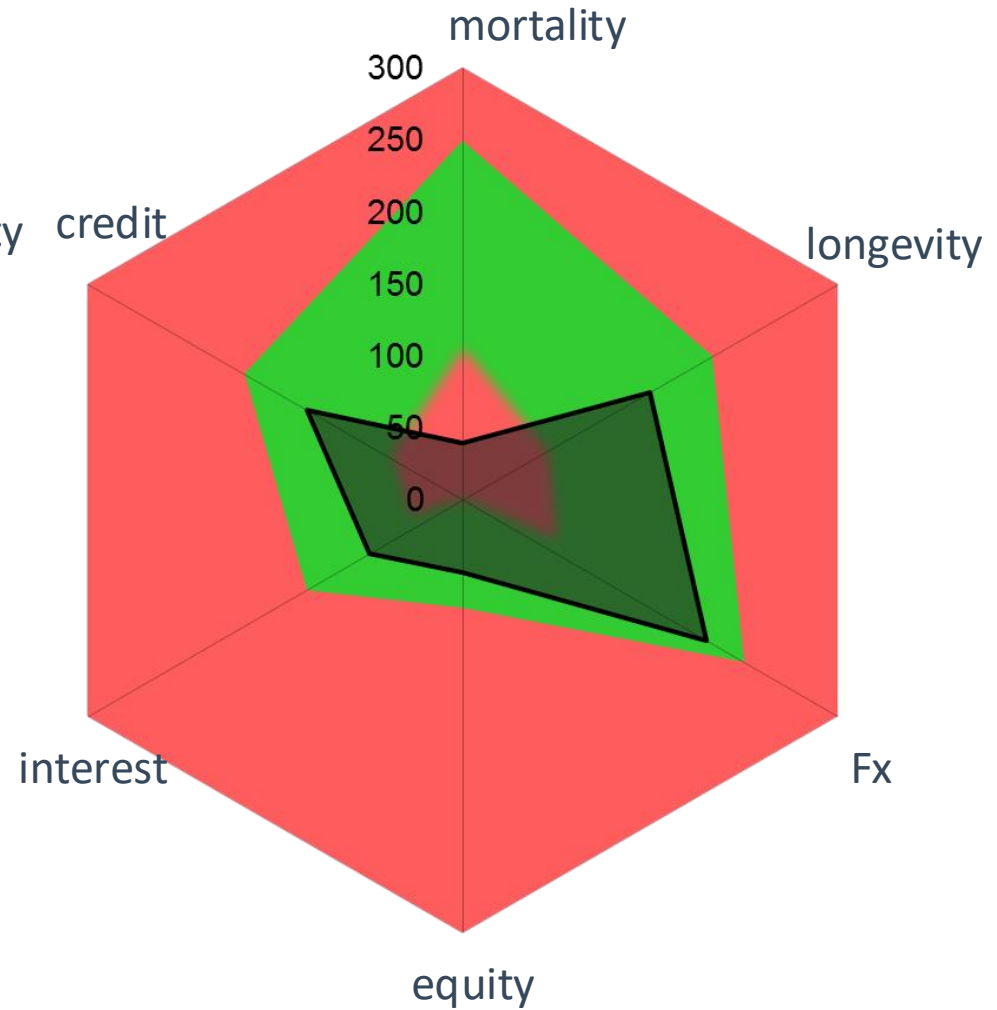
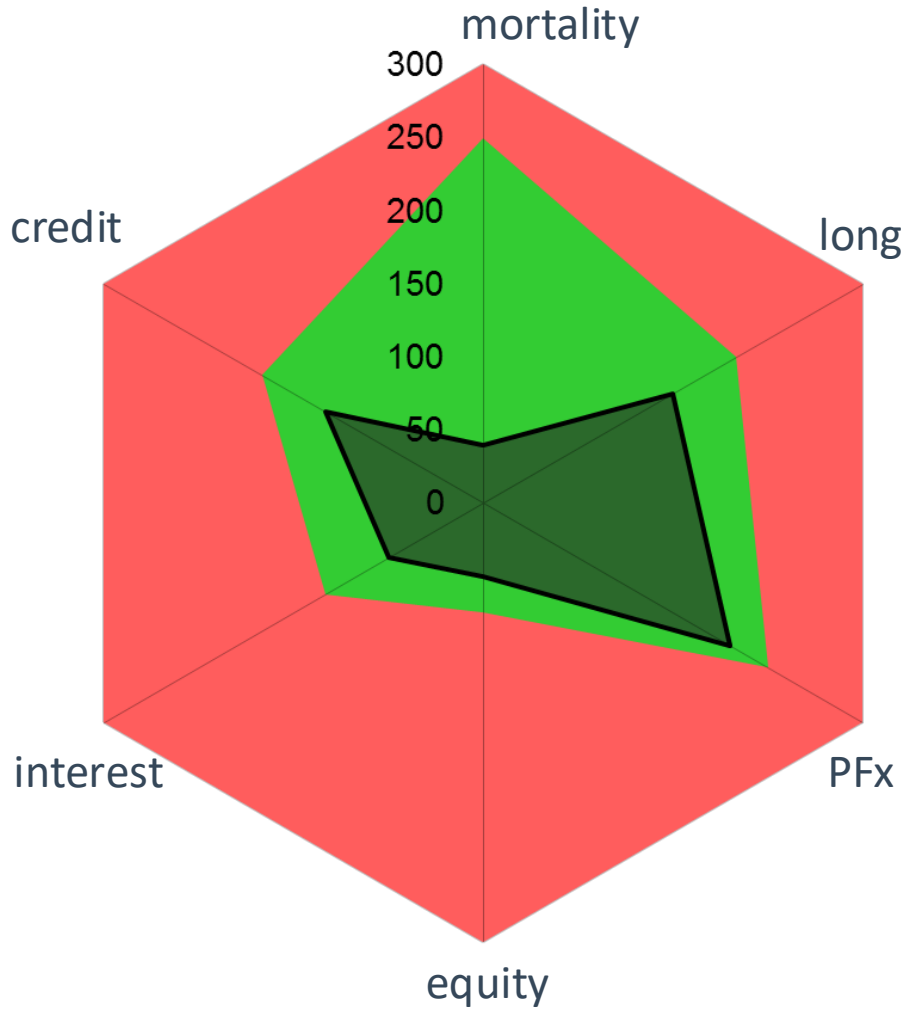
Risk Appetite Design



Risk Appetite Design



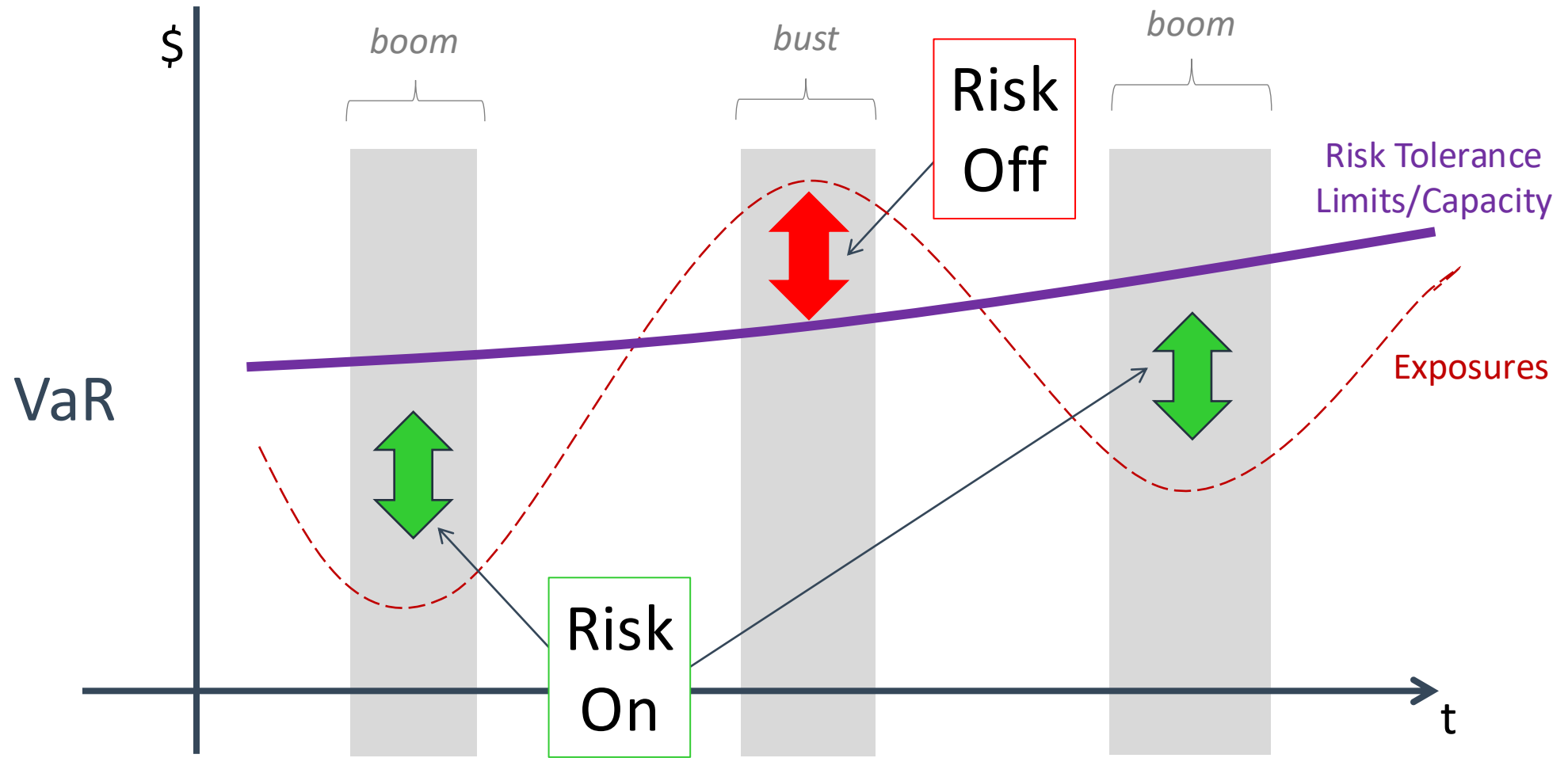
Risk Appetite Design



Case Study Exercise: Traduro SL

- What is management's risk appetite for currency risk?
- Is it appropriate?
- What is the range of expansion and financing options?
- What risk actions should accompany each and what are implications of these actions?
- What is the preferred strategy and why?

Managing Inherent Pro-cyclicality



Lunch



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: **Risk Culture**

Gerard McDonald, Executive Consultant, GRI

May 27, 2026

Agenda

- What is Risk Culture?
- Why does Risk Culture matter?
- How does Risk Culture work?
- What are the traditional issues with Risk Culture?
- How can you improve Risk Culture?



What do you think Risk Culture is?

What is Risk Culture?

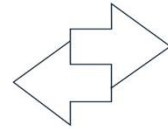


Risk culture can be understood as having ten dimensions, covered under four topics.

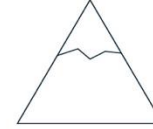
Acknowledgement



Confidence
An assured understanding of an organization’s exposure to risk without any false sense of security

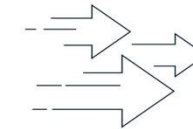


Openness
The degree to which management and employees exchange bad news or learnings from mistakes



Challenge
Scrutiny of the quality, appropriateness, and accuracy of others’ attitudes, ideas, and actions

Responsiveness



Speed of response
Perception of external changes and reaction speed to innovation or change



Level of care
Responsibility to care about the outcome of actions and decisions

Transparency



Communication
The degree to which warning signs of both internal and external risks are shared



Tolerance
Understanding of risk appetite and its linkage to overall strategy and decision making



Level of insight
Identification and understanding of risks present in the business

Respect



Adherence to rules
Alignment of individuals’ risk appetites to the organization’s



Cooperation
Consideration of broader organizational consequences and impact on overall risk appetite when any one team acts or makes decisions

Supervisory Definition of Risk Culture

OSFI definition of culture

‘Culture’ refers to the commonly held values, mindsets, beliefs and assumptions that guide both what is important and how people should behave in an organization.

Definition and development of the desired culture should include:

- Clear articulation of the desired culture, including expected behaviours and values;
- Alignment to its purpose, vision, strategy and enterprise risk management approach;
- Consideration of key talent and people management strategies;
- Consideration of policies, processes, practices and systems needed to support the desired culture;
- Implementation of frameworks, mandates and objectives that reinforce accountabilities; and,
- Proactive management of culture and behaviour risks through monitoring, assessment and reporting to support ongoing oversight and continuous improvement.

Why does Risk Culture Matter?

“Culture eats strategy for breakfast”

Dr. Peter F. Drucker

“...development of a ‘risk culture’ throughout the firm is perhaps the most fundamental tool for effective risk management.”

IIF, 2008

“Weaknesses in risk culture are often considered a root cause of the global financial crisis, headline risk and compliance events.”

FSB, 2014

Culture Matters

Organizational culture is recognized by regulators as a core supervisory concern

Culture can undermine governance even when formal controls appear strong.

Cultural weaknesses can act as leading indicators of financial distress but typically remain invisible until crises occur.

Effective supervision of culture requires clearer methodologies, stronger tools, international coordination and disciplined discretion on the part of supervisors.

Risk Culture: From Principles to Practice

*“Culture is where governance works
or fails in practice.”¹*

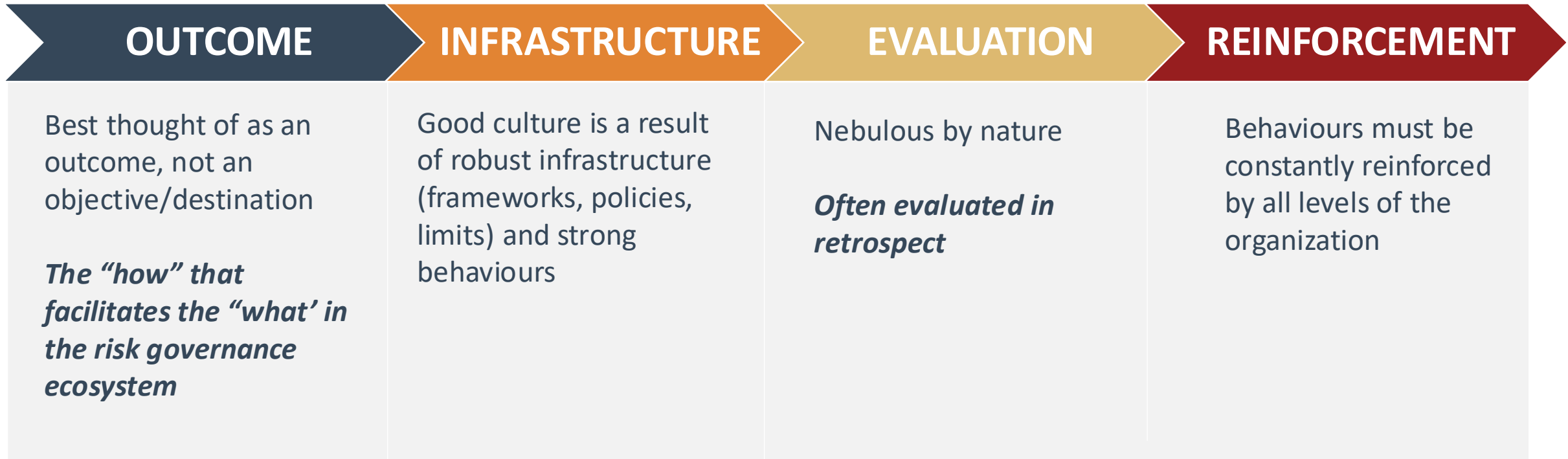
Sarah Dahlgren, Past-Head of Supervision, NY Fed

*“Prudential non-financial risks
related to governance and culture, if
left untended, could become financial
risks.”²*

Peter Routledge, Superintendent, OSFI



The What and How



Risk Culture: Foundations

Common risk language
(Risk taxonomy)

Clarity on roles and responsibilities
(Especially 1LOD risk vs 2LOD)

Robust control environment

Tone from top and middle

Strong mechanisms to consistently report and assess conduct that may be inconsistent with a strong culture

Traps and Pitfalls



Complacency

Uneven conduct standards or enforcement

- Unwilling to hold "key" employees accountable

Absence of governance and reporting on conduct

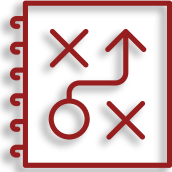
- Leads to blind spots for Board and senior management

KRIs are difficult to draft and calibrate

- Data are sparse and sometimes confidential

Organizational expansion or renewal

Lessons Learned



Can be very difficult to course correct

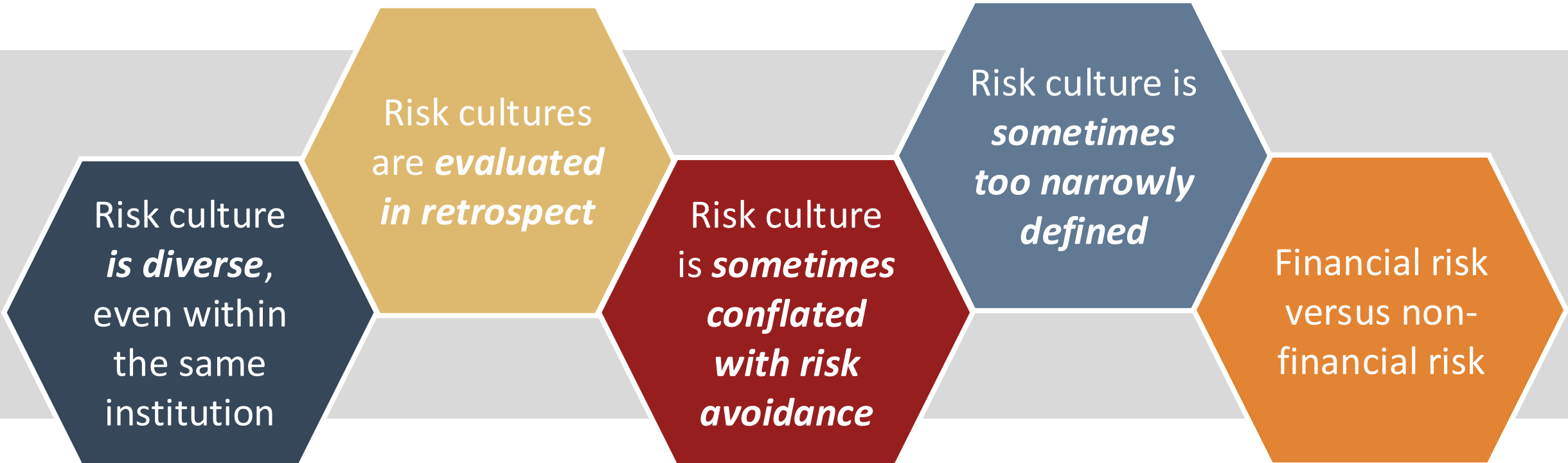


Perception of a “poor risk culture” can be very hard to shake



Mergers or acquisitions of teams can be accretive or detrimental to culture

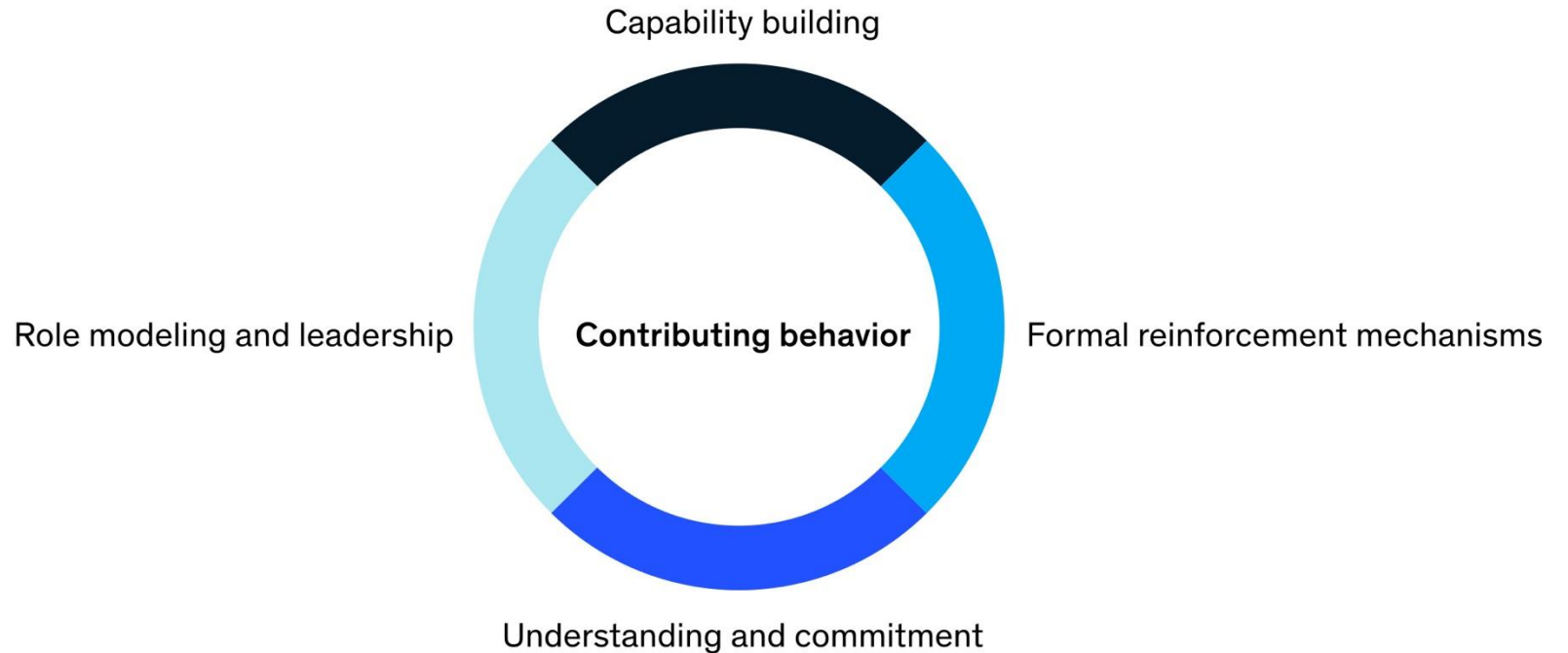
Combining Risk Cultures



How can you improve Risk Culture?

The ‘influence model’ defines four dimensions of risk-culture-change programs, ensuring that a breadth of approaches are used.

Influence model for risk-culture change



“I have the skills to behave in the new way”

“Systems reinforce desired change”

“I know what I need to change, and I want to do it”

“I see my leaders behaving differently”

Ways to improve Risk Culture

- Everyone is a Risk Manager!
- Own the Risk Culture
- Build Shared Context
- Foster Constructive Challenge
- Be Courageous!
- Model Leadership Behaviours
- Continuous Professional Development

Thank you!

Risk Oversight and Insight: A Board Perspective

Sonia Baxendale
President & CEO, GRI



**GLOBAL
RISK**
INSTITUTE