



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program

Vancouver

June 2, 2026

An Executive Perspective – Fireside Chat

Ritu Linfoot
Vice President
Enterprise Risk Management
Vancity



Break



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: ROS Overview and Macro Landscape

Jorge Cruz Lopez
Senior Research Fellow

May 27, 2026

Agenda

- **GRI Risk Outlook Survey 2026**
- **Global Macroeconomic Risks and Opportunities**

Risk Outlook Survey 2026

“We’re dealing with more uncertainty than we’ve seen in a long time, and it’s coming from multiple directions at once.”

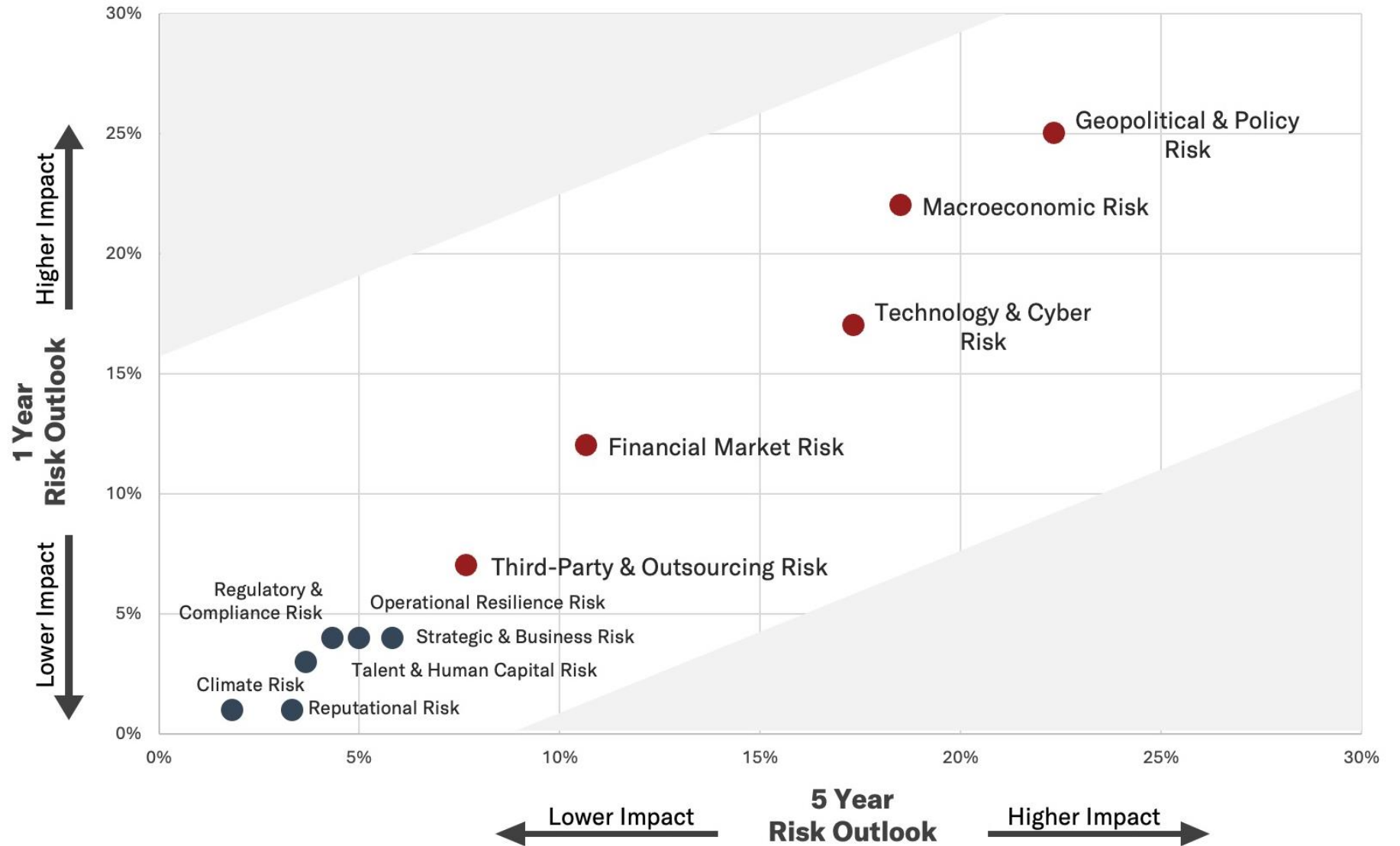
CRO Ranking of Short-term Risks

Rank	2026	2025	2024	2023	2022
#1	Geopolitical & Policy	Technology & Cyber	Technology & Cyber	Technology & Cyber	Technology & Cyber
#2	Macroeconomic	Geopolitical & Policy	Financial Market	Macroeconomic	Macroeconomic
#3	Technology & Cyber	Macroeconomic	Macroeconomic	Financial Market	Financial Market
#4	Financial Market	Financial Market	Geopolitical & Policy	Geopolitical & Policy	Climate
#5	Third-Party & Outsourcing	Third-Party & Outsourcing	Climate	Talent & Human Capital	Strategic & Business

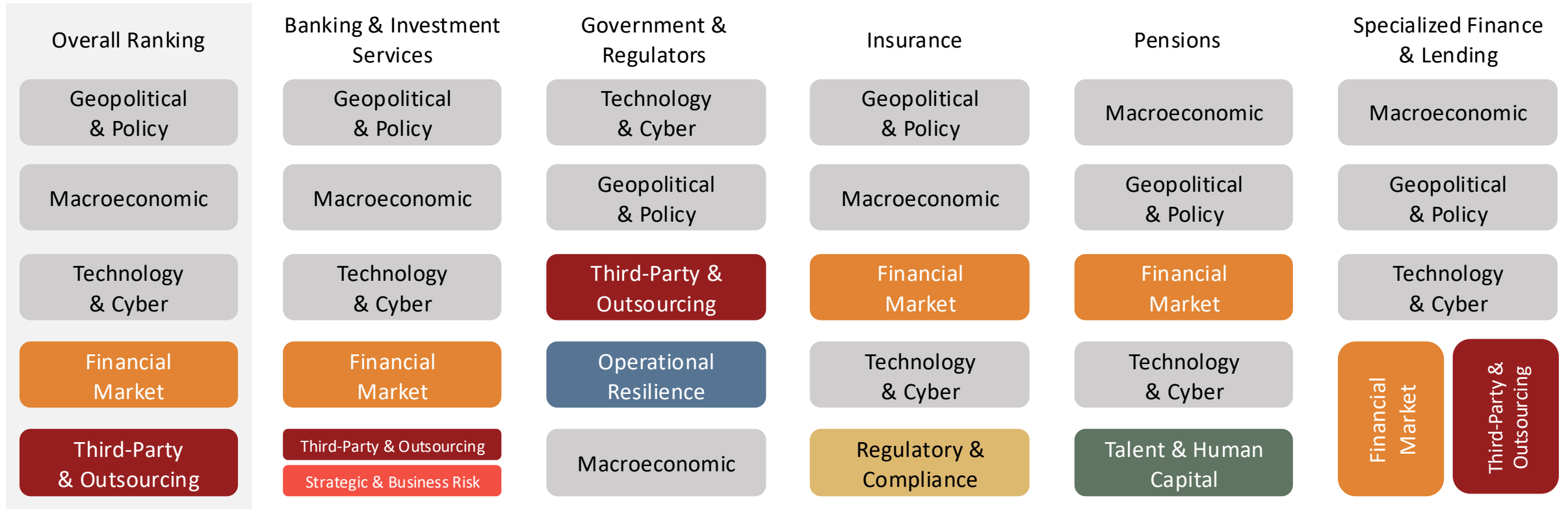
Ranking of Short and Medium-term Risks

Medium-term Shift: From Immediate Exposure to Strategic Sustainability

Over the five-year outlook, respondents place relatively greater emphasis on risks that shape business model resilience and long-term competitiveness.



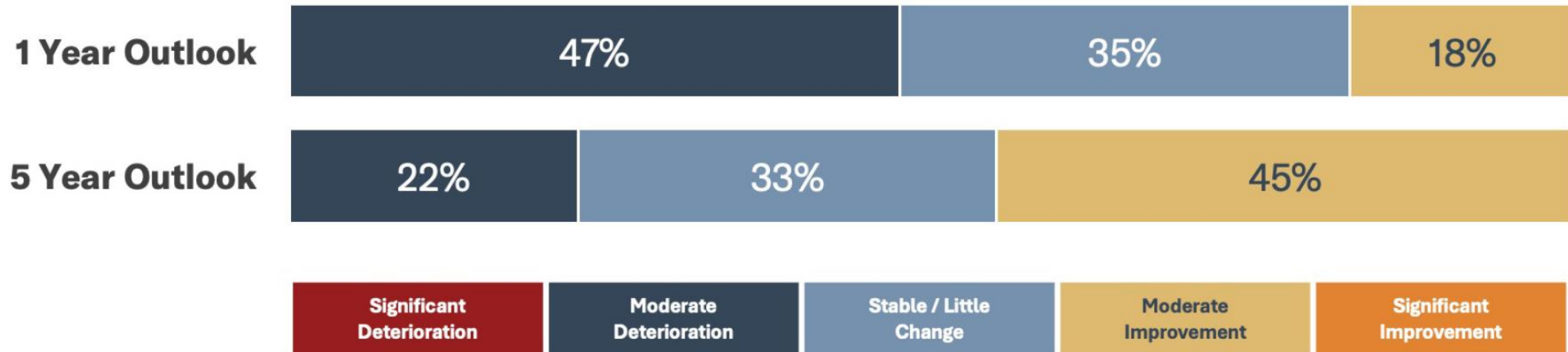
Ranking of Short-term Risks by Segment



Outlook for the Canadian Financial Sector

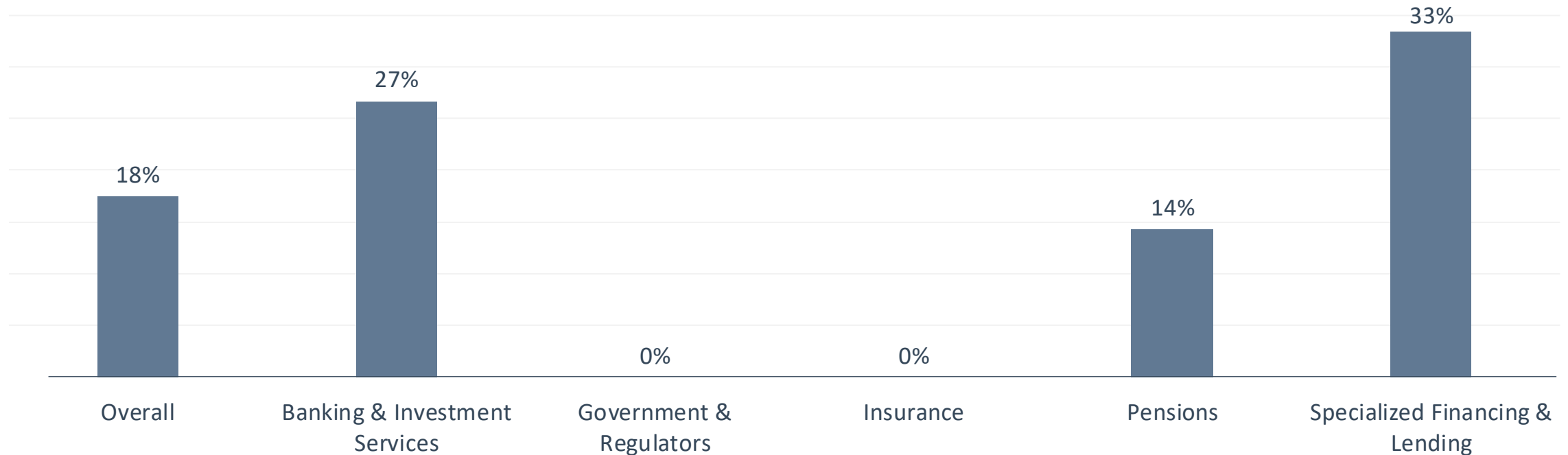
Respondents distinguish between immediate pressures and longer-term sector resilience, suggesting that uncertainty is viewed as persistent but manageable.

A Cautious Short-Term Outlook, Paired with Greater Medium-Term Optimism



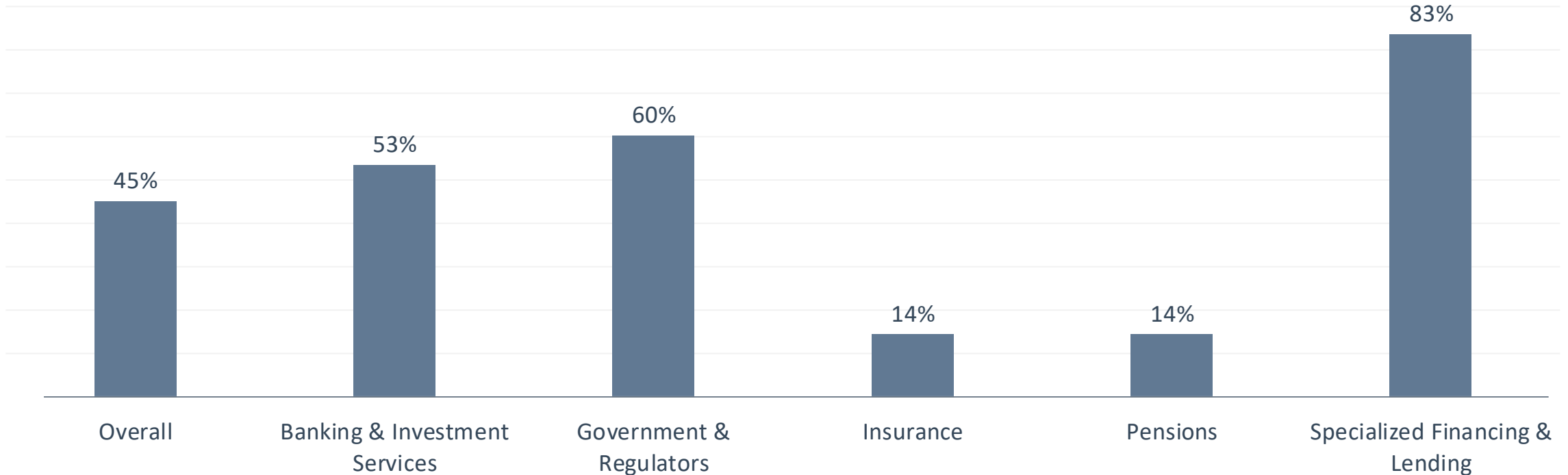
Outlook for the Canadian Financial Sector

0% of Government & Regulators respondents see moderate to significant improvement for the sector in the short term



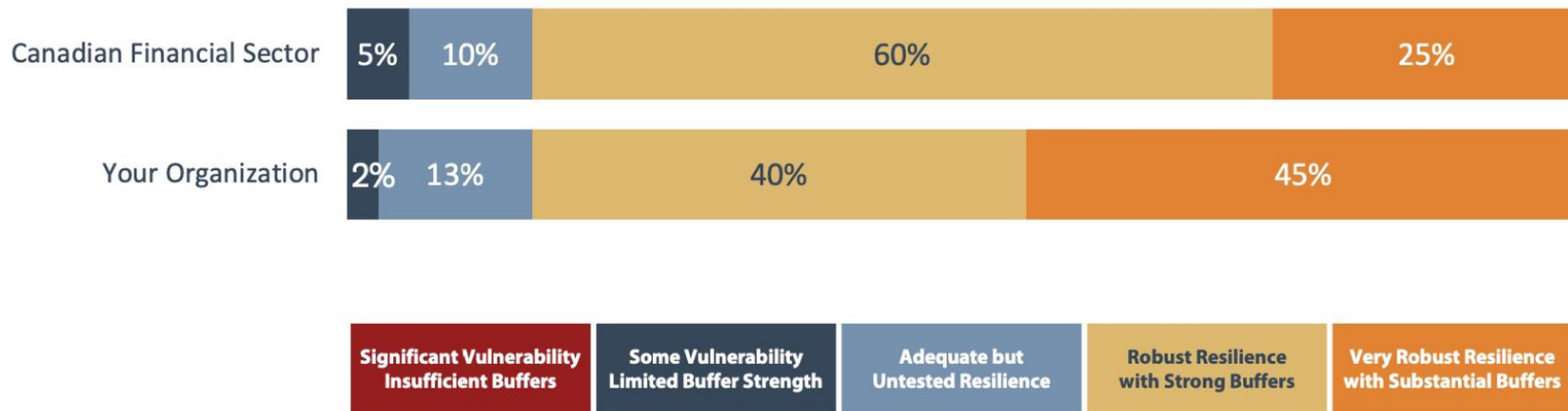
Outlook for the Canadian Financial Sector

*This improves to 60% in the medium term for the segment –
% respondents see moderate to significant improvement for the sector*



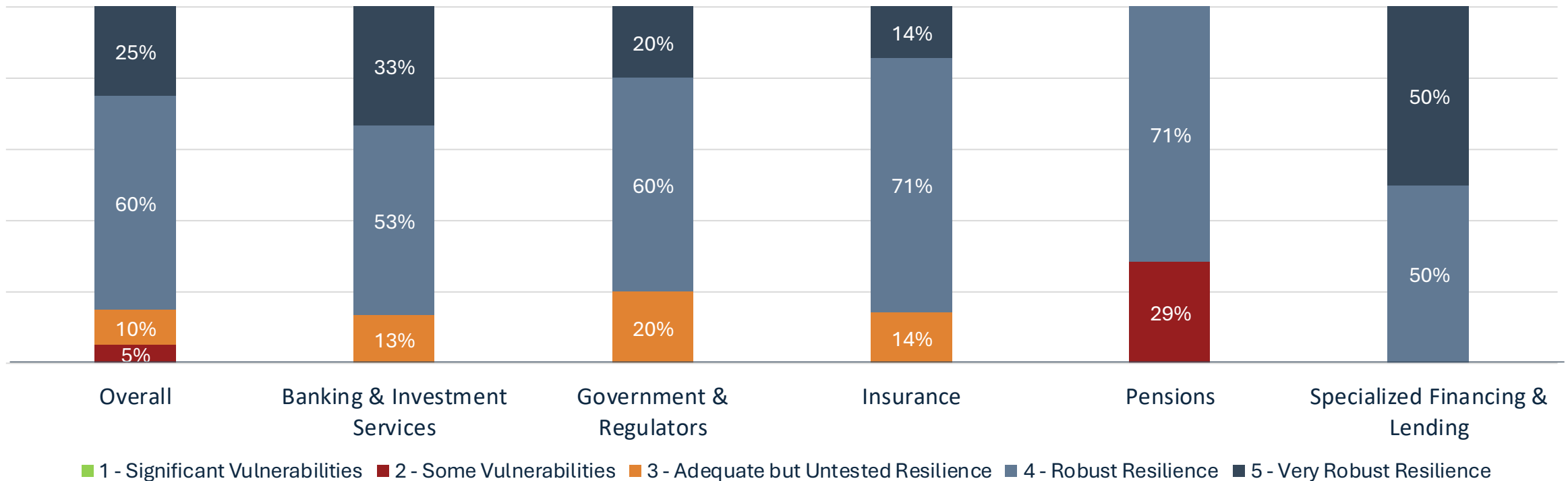
Ability to Withstand a Severe Shock Over the Next Year

Confidence in organizational resilience exceeds confidence in sector-wide resilience, highlighting the limits of organizational-level control in an externally driven risk environment.

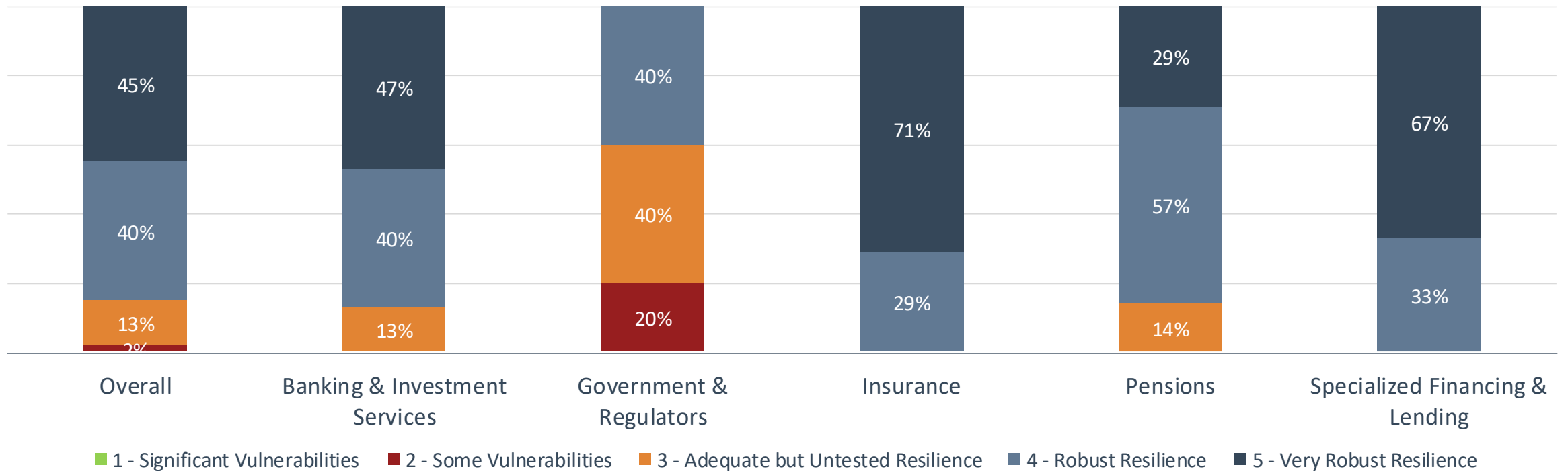


“We are navigating uncertainty rather than responding to clearly defined shocks.”

Canadian Financial Sector: Ability to Withstand Severe Shock

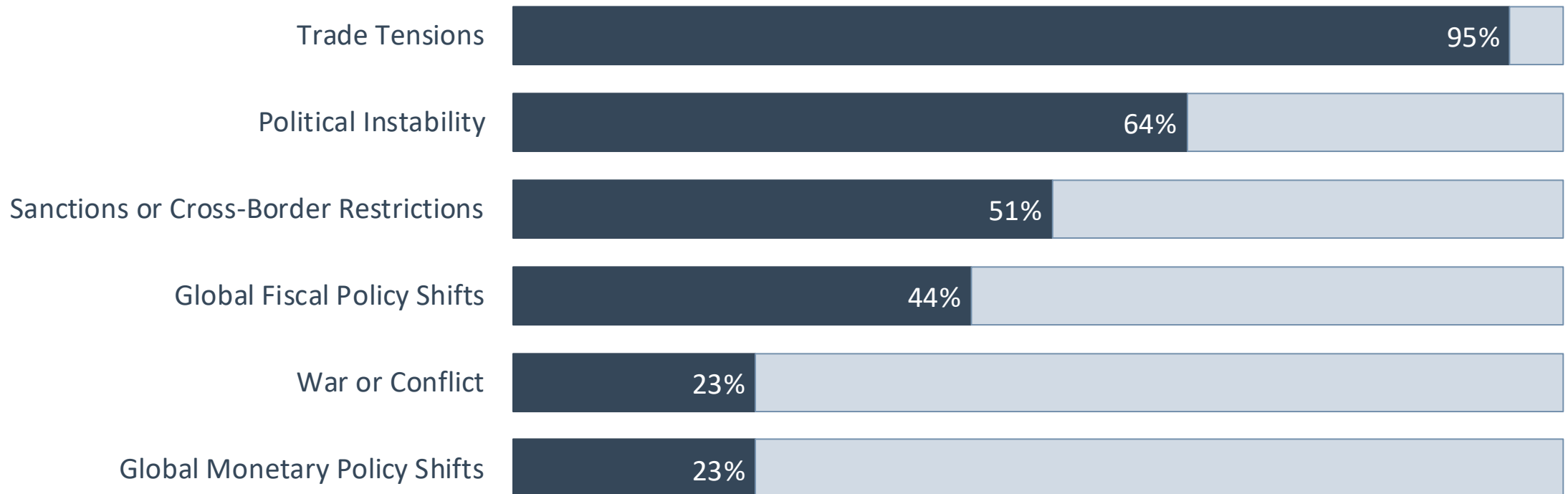


Your Organization's Ability to Withstand Severe Shock



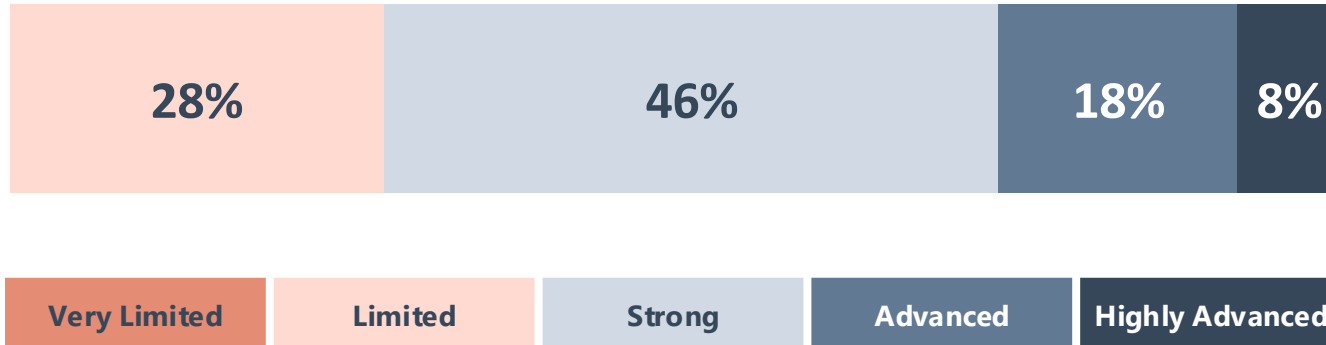
Geopolitical & Policy Risk

When asked for their top three concerns, respondents identified trade tensions, political instability, sanctions and global policy shifts as the most significant contributors to geopolitical and policy risk.



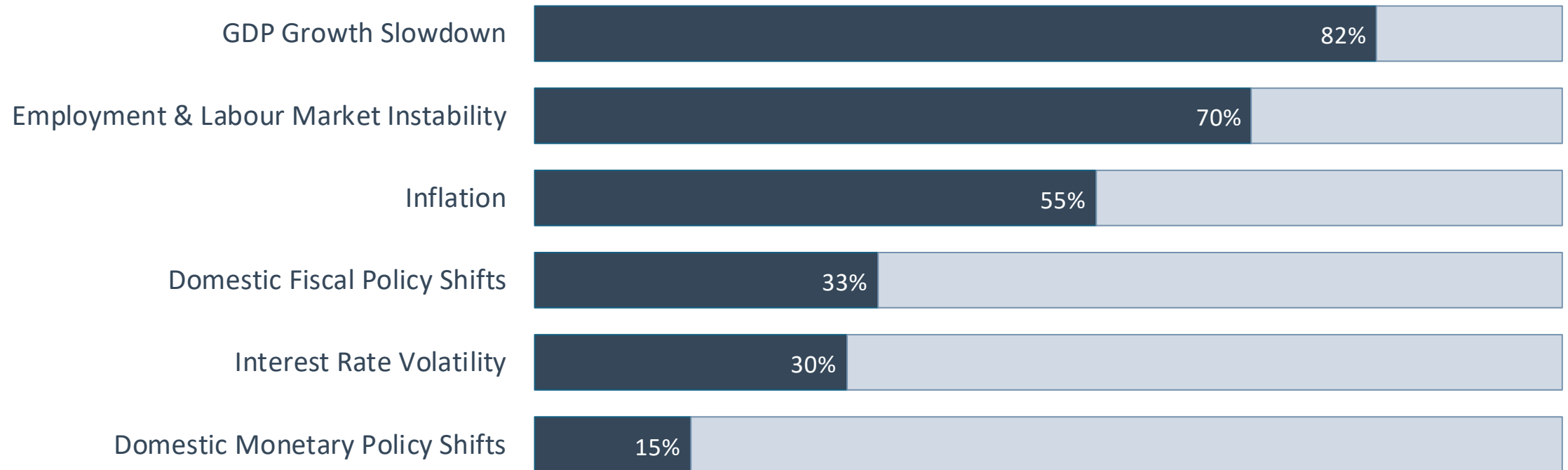
Geopolitical & Policy Risk

How would you rate your organization's ability to detect, prevent, and respond to geopolitical and policy risks?



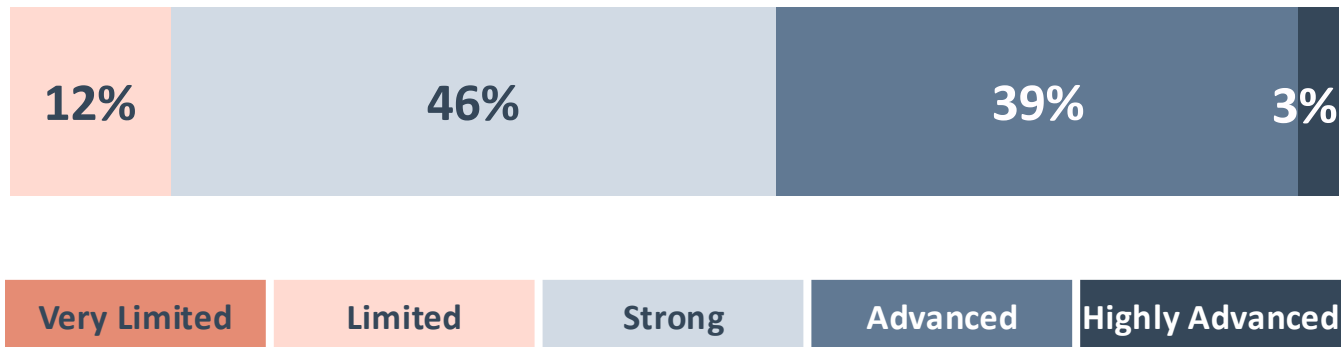
Macroeconomic Risk

When asked for their top three concerns, respondents identified GDP slowdown, labour market instability, and inflation as the most significant contributors to macroeconomic risk.



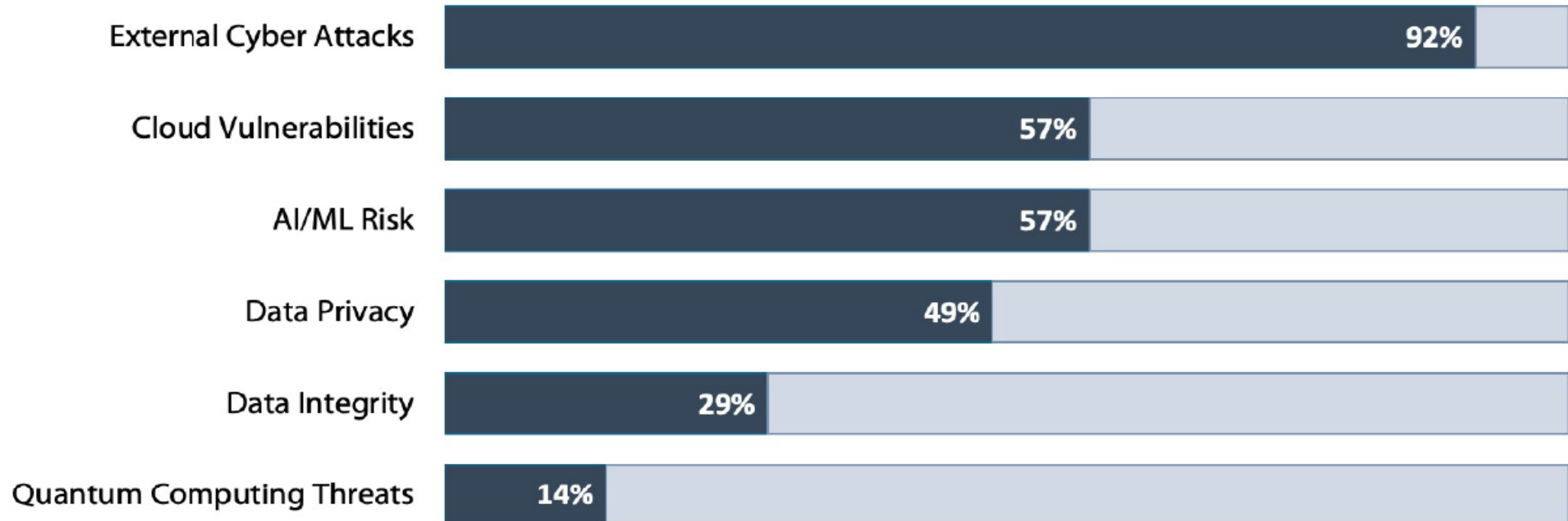
Macroeconomic Risk

How would you rate your organization's ability to detect, prevent, and respond to macroeconomic risks?



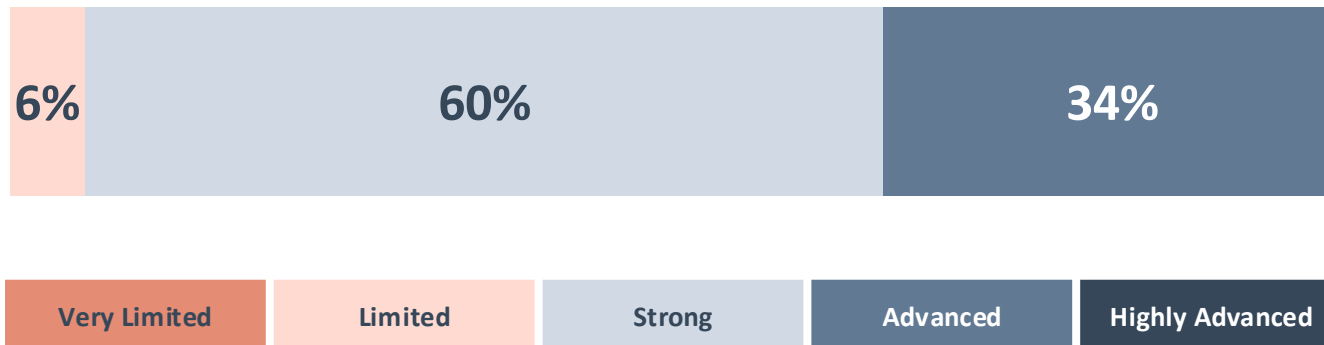
Technology and Cyber Risk

When asked for their top three concerns, external cyber attacks, cloud vulnerabilities and AI-related risks dominate respondents' technology and cyber risk concerns.



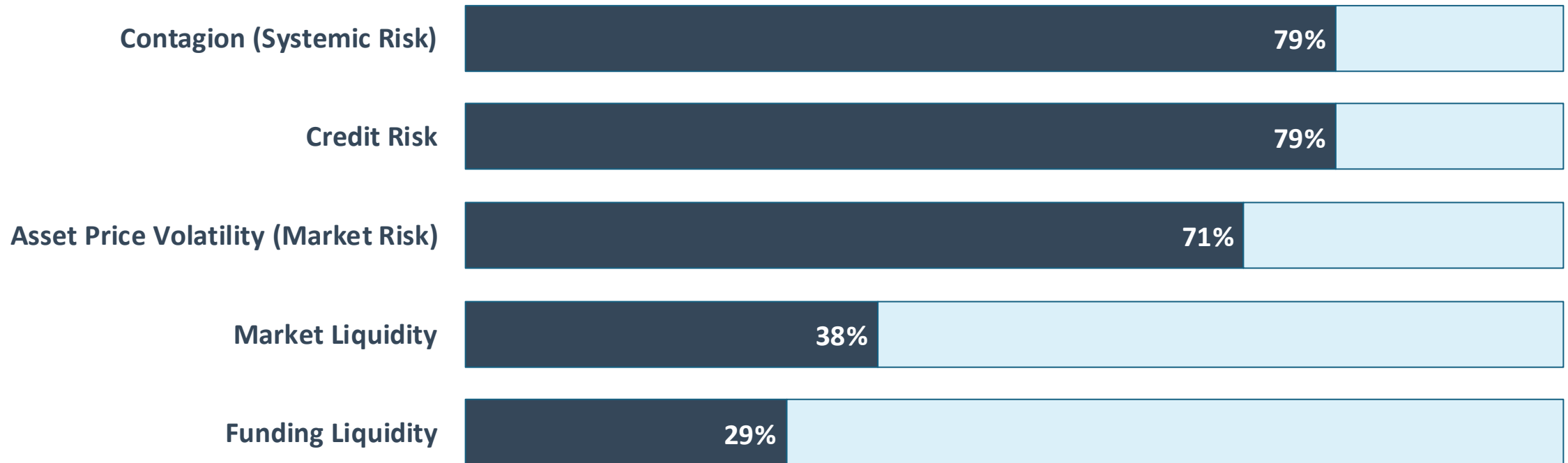
Technology and Cyber Risk

How would you rate your organization's ability to detect, prevent, and respond to cyber and technology-related risks?



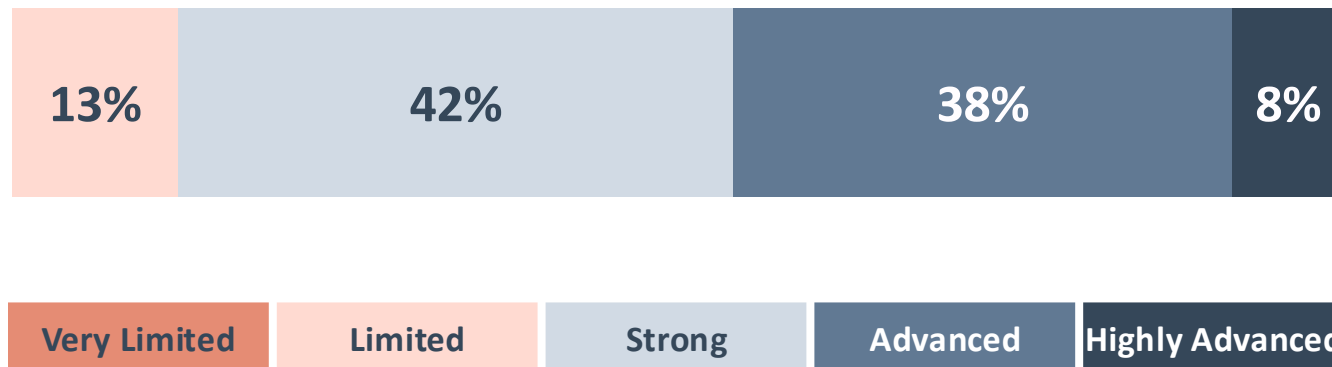
Financial Market Risk

When asked for their top three concerns, respondents identified contagion (systemic), credit, and asset price volatility (market) as the most significant contributors to financial market risk.



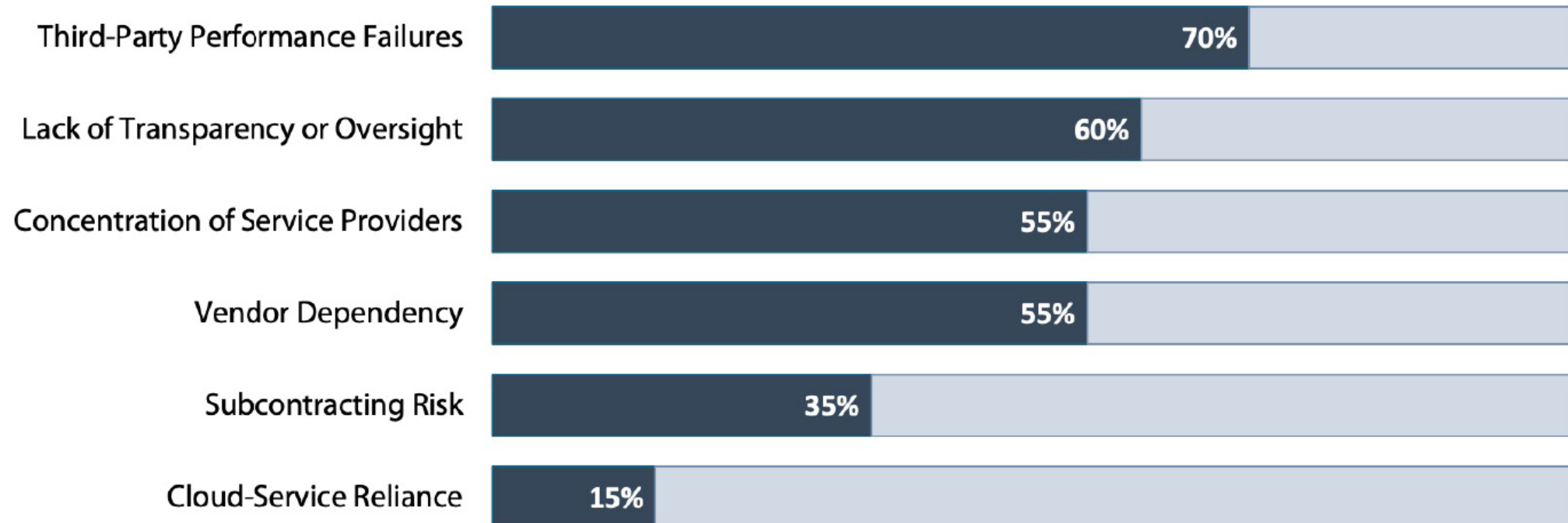
Financial Market Risk

How would you rate your organization's capacity to measure and monitor financial market risks in real time?



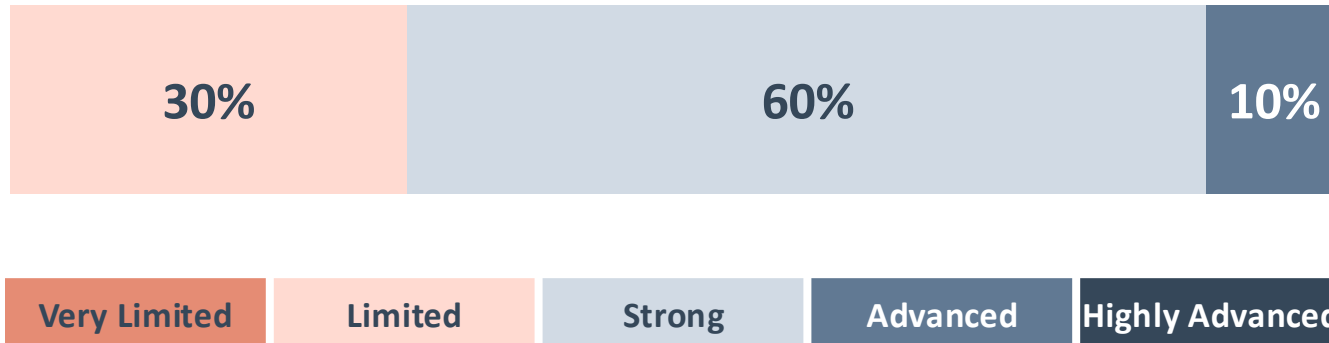
Third-party and Outsourcing Risk

When asked for their top three concerns, respondents identified third-party failures, lack of transparency/oversight, concentration risk, and vendor dependency are the most frequently cited third-party risk concerns.



Third-party and Outsourcing Risk

How would you rate your organization's ability to monitor, assess, and govern third-party risks?



Global Macroeconomic Risks & Opportunities



Global Macroeconomic Landscape: Fragile Stability

We are operating in a “fragile equilibrium” macro environment

Inflation & Interest Rate Transition

- Inflation is coming down globally, but trends are uneven and fragile
- Central banks facing **higher-for-longer uncertainty**

Monetary Policy Divergence

- U.S. growth remains relatively strong → delays easing
- Europe weaker → more pressure to cut rates
- China structurally slowing → deflationary impulse
- Currency and capital flow volatility
- **Result:** policy uncertainty → volatility in rates and asset prices

Global Macroeconomic Landscape: Fragile Stability

Geopolitical Fragmentation

- Trade reconfiguration, sanctions, supply chain realignment → inflation
- Shift from efficiency → resilience in global supply chains
- Rise of “friend-shoring” and strategic blocs

Debt & Fiscal Pressures

- Elevated sovereign debt limiting policy flexibility

Energy & Commodity Volatility

- Conflict-driven supply risks (Middle East focus)
- Persistent inflationary tail risks

Spillovers: Iran War and Global Macro Transmission

*The Iran conflict matters not just geopolitically, but macroeconomically through **spillover channels***

Energy Shock Risk

- Oil supply disruption (Hormuz chokepoint)
- Shipping & insurance costs rising
- Energy markets as a transmission channel of systemic risk

Inflation Reacceleration Risk

- Energy → transportation → broad price pressures
- Delays central bank easing cycles.
- Risk of **stagflation** and damaging central bank credibility

Spillovers: Iran War and Global Macro Transmission

Financial Market Volatility

- Flight to safety (USD, U.S. Treasuries)
- Equity and credit repricing

Policy Constraints

- Central banks: inflation vs. recession trade-off
- Governments: fiscal strain + defence spending

Tail Risks

- Regional escalation → global growth shock
- Cyber and hybrid warfare spillovers
- Energy + financial system shock simultaneously
- This is a **classic polycrisis trigger**

Canadian Macro Outlook

Canada is exposed to global forces, while facing domestic constraints

Growth & Household Vulnerability

- Slowing growth, high household debt
- Interest rate sensitivity remains elevated

Housing Market Sensitivity

- Housing remains a **core macro channel for systemic risk**
- Mortgage renewals at higher rates
- Risk to consumption and financial stability

Canadian Macro Outlook

Inflation & Bank of Canada Path

- Inflation moderating but not fully anchored (above target risks persist)
- Policy easing contingent on global conditions
- External shocks (particularly energy) matter significantly
 - Canada may benefit from exports
 - But inflation could delay rate cuts

External Exposure

- Energy exports → upside from global shocks
- Trade dependence on U.S. cycle

The Macro Outlook: Risks and Opportunities

The current macro environment creates a **mixed outlook** with risks and opportunities, where **liquidity and diversification** have become more important

Risks:

- Increased volatility across asset classes
- Correlated drawdowns (equities + bonds under stress)
- Liquidity stress in private markets
- Counterparty and credit risk

Opportunities:

- Higher long-term yields → improved fixed income return outlook
- Dislocations → opportunities in private markets and infrastructure
- Illiquidity premium remains attractive
- Real assets (energy, infrastructure) can benefit from macro/geopolitical shifts



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: Technology Disruption and Risk

Agentic AI, Quantum Computing, and Emerging Industry Insights

Jorge Cruz Lopez
Senior Research Fellow

June 2, 2026

Agenda

1. **Agentic AI**
2. **Quantum Computing**
3. **Emerging Industry Insights (FIFAI)**
4. **Case Study**

1. Agentic AI

“The question shifts from ‘Is the model accurate?’ to ‘Who’s accountable when the system acts?’ ... Agency isn’t a feature; it’s a transfer of decision rights.”

Rich Isenberg, Partner, McKinsey & Company, 2026

What is Agentic AI, How is it Different, and Why Does it Matter?

Agentic AI refers to systems that **can autonomously plan, decide, act and adapt to achieve goals** (often by orchestrating multiple tools, models, and processes without continuous human direction).

From AI as advisor → AI as actor (delegated decision-making)

- The transition is happening faster than many governance frameworks expect, driven by:
 - Multi-agent architectures
 - Tool-use (APIs, code execution, system access)
 - The fact it learns and adapts in real time
- **Operates across systems**, vendors, and data sources and compresses **decision cycles** from days to minutes (or seconds).
- Shifts risk **from model outputs to model behavior**.
- The risk **profile changes fundamentally**: failures are no longer single-point errors but cascading, fast-moving events.
- The key issue is not just *additional intelligence*; it is **autonomy at scale**.

Agentic AI: A Risk Multiplier?

Agentic AI can accelerate and amplify existing risks:

- **Operational:** Automated actions propagate errors across systems at speed.
- **Cyber:** Agents can autonomously scan, exploit, and escalate vulnerabilities.
- **Third-Party:** Agents act through vendors, platforms, and shared infrastructure.
- **Governance:** Accountability gaps (who approves, who audits, who stops the agent?).
- **Systemic:** Many institutions adopting similar agents → correlated failure modes.

For many financial institutions: The exposure can also be indirect but material (e.g., through custodians, counterparties, clearing systems, and market infrastructure)

Agentic AI as a Systemic, Grey-to-Black Swan Risk

Agentic AI can also introduce new (often non-linear) risks:

- **New risk profile:** Speed, scale, autonomy and coordination risks exceed human oversight capacity and compound due to tightly coupled financial systems.
- **Traditional controls:** Model validation, periodic reviews, human approvals, etc. can lag behind agentic behavior.
- **Key failure modes:** Goal misalignment, emergent collusion, rapid error propagation.
- **Systemic exposure:** Financial markets, critical infrastructure, cyber physical systems.
- **Grey Swan dynamics:** Known possibility, uncertain timing, unclear blast radius.
- **Black Swan potential:** Cascading failures from tightly coupled AI driven systems.

Agentic AI is not just a **new technology risk vector**.
It is also a **risk multiplier** that reshapes how shocks propagate through
economic and geopolitical systems.

Anthropic's Claude Mythos

What is Mythos (Claude Mythos Preview)?

- Anthropic's most advanced frontier AI model.
- Can autonomously identify and exploit software vulnerabilities at a speed and scale beyond human capability.

In controlled testing: discovered thousands of high-severity and zero-day vulnerabilities across every major operating system and web browser, many decades old.

- Because of its dual-use cyber capability, Anthropic has withheld public release, granting access only to ~40 trusted organizations under **Project Glasswing**, including major banks and critical infrastructure providers.

Anthropic's Claude Mythos

Key Risks for Financial Institutions

Systemic Cyber Risk:

- Compress multi-month cyberattacks into hours.
- Increase the risk of simultaneous failures across interconnected financial systems.
- Increased N-Party Risk: Custodians, asset managers, clearing houses, and insurers.
- Could trigger liquidity freezes, valuation disruption, and counterparty failures.
- Increases vulnerability of legacy infrastructure embedded in market plumbing.

Model Control & Governance Risk:

- Anthropic experienced unauthorized access via third-party vendors → control failures may lie outside core systems.
- Raises fiduciary questions: Who controls frontier AI, who audits it, and who bears loss if containment fails?

Anthropic's Claude Mythos

Strategic Opportunities

Defensive and Strategic Advantage

- Can help identify latent vulnerabilities before adversaries do.
- Early access by banks illustrates a first-mover security advantage.

Investments & Stewardship

- Cybersecurity platforms.
- Resilience-focused infrastructure.
- AI safety and assurance market.
- Portfolio stress-testing (cyber risk and macro-financial shocks).

Anthropic's Claude Mythos

What Comes Next

- **Containment phase (2026):** Restricted deployment, regulator briefings, and emergency cyber coordination across banks and insurers.
- **Diffusion risk:** Comparable models will emerge elsewhere; withholding is temporary, not a permanent solution.
- **Expectation shift:** Cyber resilience becomes a core fiduciary responsibility, not just an IT function.

2. Quantum Computing

“For financial institutions, quantum computing represents both an opportunity and a threat.”

*GRI’s Quantum Computing Primer
for Financial Sector Executives, 2026*

What makes quantum computing different?

Opportunities:

Complex calculations can be processed exponentially faster than before



Substantial advancements in areas like:

- Portfolio optimization
- Simulations
- Modeling
- Liquidity optimization
- Derivative pricing
- Fraud detection
- Pattern recognition



Better data analysis, decision-making, and competition

What makes quantum computing different?

Threats:

- Current encryption methods can only protect against attacks from classical computers.
- Quantum Threat Timeline = The point when quantum computing can break current cryptographic standards.
- In the hands of malicious actors, global digital infrastructure is at risk.

Preparation Should Begin Early

How long until malicious actors have access to disruptive quantum technology



The Mosca Inequality

How long a system upgrade will take

How long the data must remain secure

Preparation Should Begin Early

Most experts think it is likely there will be a disruptive quantum threat in the next 10 years

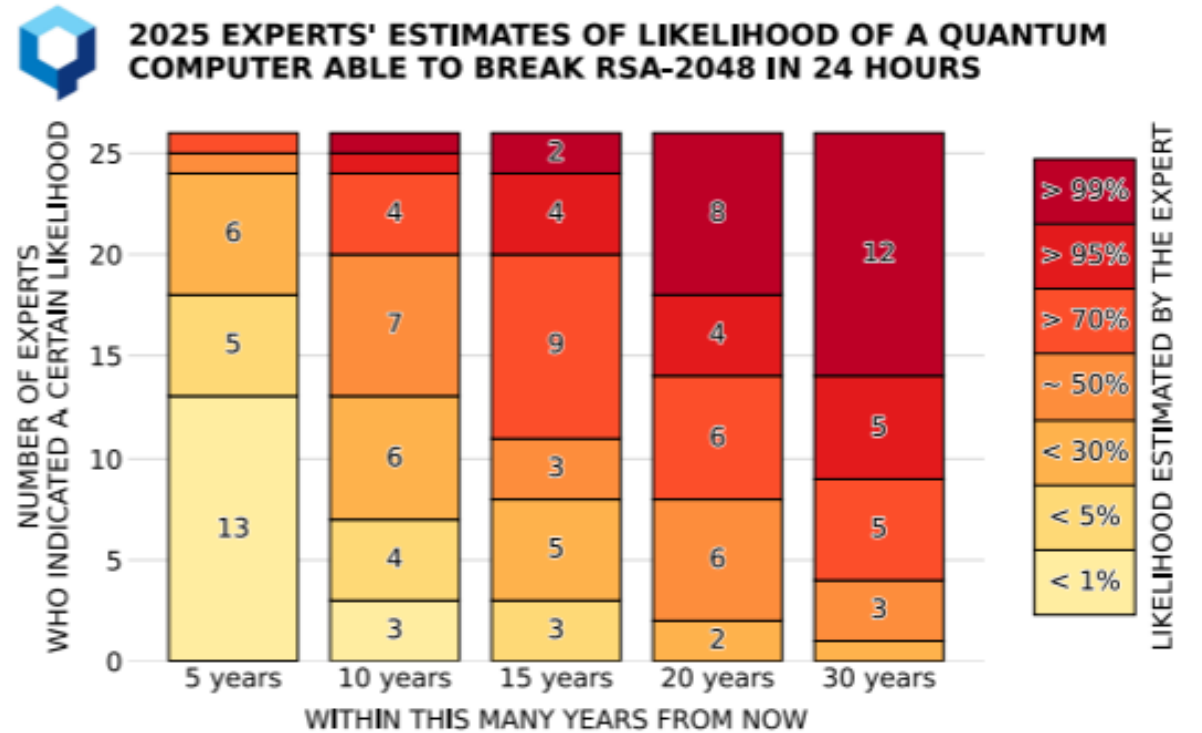


Figure 2 Experts' estimates of the likelihood of a cryptographically relevant quantum computer, aggregated by likelihood bin and timeframe.

Resisting Quantum Attacks

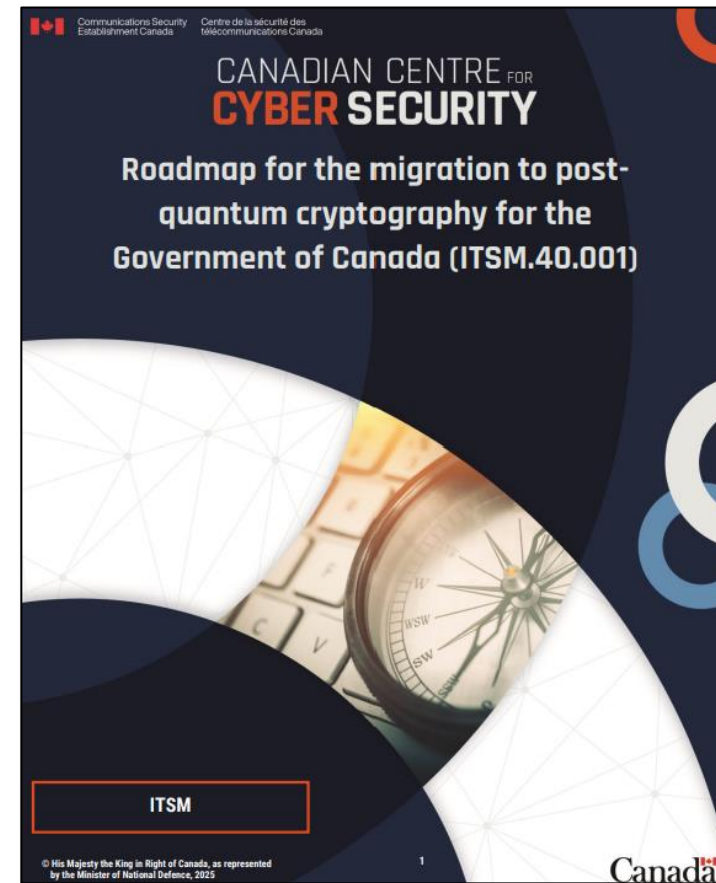
- Financial institutions will need to replace or upgrade encryption across hardware, software, networks and legacy technology environments.
- However, this work can take years to complete.

Securing data against quantum attacks cannot be treated as a last-minute technology upgrade.

Governments are Acting Now

The Canadian government released a detailed roadmap for federal IT systems last year:

- Every department must draft a *Post-Quantum Cryptography* migration plan by April 2026.
- High-priority systems must be protected by the end of 2031.



3. Emerging Industry Insights



“AI is a transformative force—both awe-inspiring and potentially perilous...Its true impact will hinge on disciplined, responsible innovation & robust collaboration across borders and sectors.”

Peter Routledge, Superintendent, OSFI

A Public and Private Collaboration

Phase 1: GRI-OSFI collaboration helped prepare for the future of regulation

- Framework to support AI implementation and oversight: EDGE Principles (Explainability, Data, Governance, and Ethics)
- *A Canadian Perspective on Responsible AI* (April 2023)

Phase 2: Four Workshops – 170 Participants – 6 Sponsors

- Deepen our understanding of how AI technologies are reshaping opportunities and threats for the financial system and financial consumers
- Discuss best practices and effective AI risk management strategies to learn how to build resilience into individual organizations, consumer well-being protections, and the financial system.
- *AI Risks and Opportunities: Adopting an AGILE Framework in Canadian Financial Services* (March 2026)



FIFAI Phase I

The output of the Forum created a series of guardrails that the industry could leverage to manage the implementation of Artificial Intelligence.

The final report, *A Canadian Perspective on Responsible AI*, was published in April 2023.

1. EXPLAINABILITY

enables institutions to **deepen trust with their customers**.
When customers understand the reason for decisions, they become empowered to work towards their goals.

2. **DATA** leveraged by AI allows institutions to **provide targeted and tailored products and services** to their customers, improve fraud detection, enhance risk analysis and management, boost operational efficiency, and improve decision making.

3. GOVERNANCE

supports the realization of AI's potential by **ensuring that the institution has the right culture, tools, and frameworks** available to support the AI lifecycle.

4. **ETHICS** encourages institutions to **consider broader societal impacts of their AI systems** and make a conscious choice of what role they would like to play in shaping the world around them.

FIFAI II Workshops



Department of Finance
Canada
Ministère des Finances
Canada



Financial Consumer
Agency of Canada
Agence de la consommation
en matière financière du Canada



Workshop 1

Security & Cyber Risk

- GRI
- OSFI
- Department of Finance

[Interim report](#)

Workshop 2

Financial Crimes

- GRI
- FINTRAC

[Interim report](#)

Workshop 3

Financial Stability

- GRI
- OSFI
- Department of Finance

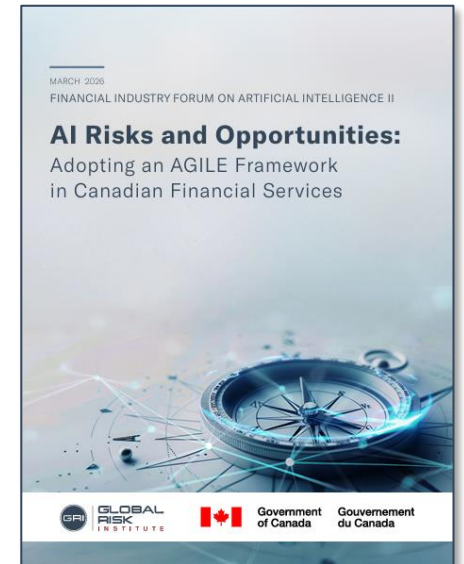
[Interim report](#)

Workshop 4

Consumer Protection

- GRI
- Financial Consumer Agency of Canada (FCAC)

[Interim report](#)



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.

FIFAI II: Areas of Evolving Impact to the Risk Environment

1. Consumer Risks

- **Trust** underpins the relationship between consumers and the financial sector. AI adoption has the potential to either strengthen that trust or undermine it.
- **Transparency, explainability and accountability** are key pillars of responsible AI, including appropriate disclosure and consent.
- **Data risk, fraud risk and access issues** can also contribute to AI risks for consumers.

FIFAI II: Areas of Evolving Impact to the Risk Environment

2. AI Enabled Security and Cyber Threats

- AI significantly **amplifies** already existing security and cybersecurity threats, like social engineering and synthetic fraud.
- AI is increasingly being **weaponized**. Cyberattacks can be easily automated, accelerated, and tailored by threat actors.
- **Disinformation/misinformation** can spread quickly due to the ubiquity of social media and the increasingly polarized environment.

FIFAI II: Areas of Evolving Impact to the Risk Environment

3. Knowledge and Talent Gaps

- FIFAI II identified “**shortage of AI talent**” as one of the top internal hurdles to managing AI-related risks.
- Participants highlighted that talent scarcity is not merely a human resources challenge but even a potentially existential threat to an institution’s ability to operate safely and competitively in an AI-dominated landscape, as well as to the industry’s regulators and supervisors.

FIFAI II: Areas of Evolving Impact to the Risk Environment

4. Third-Party Concentration and Supply Chain

- Third-party risk in the AI supply chain is a significant issue globally and for Canada's financial sector, as noted in all FIFAI II workshops.
- AI is **deepening third-party dependencies** often essential for model development, data services, and computing infrastructure.
- AI deployment is increasing the extent to which individual FIs and the sector rely upon a relatively small number of third-party technology providers, and many critical service providers operate outside the regulatory perimeter.

FIFAI II: Areas of Evolving Impact to the Risk Environment

5. Strategic Risk

- One of the most prominent themes of the workshops was that the biggest risk is **not doing enough**.
- Moving too slowly, whether due to conservative decision-making or other factors, could be just as detrimental as adopting AI too rapidly without properly managing risks.

FIFAI II: Areas to Mitigate Risks and Capture Opportunities

1. Stay ahead of AI-driven risks

- Understand how rapid AI advances, including agentic AI, reshape the risk landscape beyond internal adoption.
- Build board-level engagement, expand stress testing, and monitor systemic threats such as market volatility and AI-related credit risks.

2. Make best practices regular practice

- Embed strong governance, evergreen controls, and data integrity standards.
- Keep humans in the loop for high-impact decisions, ensure transparency and consumer rights, and strengthen third-party oversight.
- Build repeatable safeguards that adapt as AI evolves.

FIFAI II: Areas to Mitigate Risks and Capture Opportunities

3. Adopt an AI growth mindset

- AI is more than efficiency; it is a catalyst for growth, resilience and competitiveness.
- Invest boldly in talent, modern infrastructure and responsible innovation to deliver better products, stronger defenses and improved customer experiences.

4. Build AI skills at every level

- Invest in continuous training for boards, managers and technical teams. Create collaborative and adaptive learning ecosystems.
- Empower consumers with AI literacy to protect themselves and make informed choices.

5. Strengthen system-wide defenses against AI risks

- Collaborate across industry, regulators and government to set common standards, improve third-party oversight and increase regulatory certainty in AI.
- Improve digital ID security, expand real-time threat sharing and upgrade incident response frameworks to protect financial stability in the AI era.

4. Case Study

WhitePine Financial Holdings: AI as a Cross-Cutting Risk

Fictional illustration prepared for discussion purposes

WhitePine Financial: AI as a Cross-Cutting Risk

Case Summary:

- Canadian financial institution (banking, lending, wealth, insurance)
- Rapid AI adoption across core functions (2024–2026)
- **Three events raise concern:**
 - 1. Credit platform (ML):** Unexpected declines + higher pricing vs policy; rising complaints
 - 2. Call centre assistant (GenAI):** Confident but incorrect customer advice; weak traceability
 - 3. Cash management (Agentic AI):** Autonomous liquidity decisions; failed human overrides
- Each function operated “within mandate”
- Regulators already engaged (OSFI, FCAC)

WhitePine Financial: AI as a Cross-Cutting Risk

What's Really Going On? - From Isolated Incidents to a Systemic Risk Pattern

- This is NOT three separate issues:
 - Not just **model risk**
 - Model “correctness” ≠ business “appropriateness”
 - Not just **conduct / consumer protection**
 - Frameworks detected complaints, not systematic harm
 - Not just **operational breakdown**
 - Control existed in theory, not in practice
- This is a failure to govern AI as an end-to-end system
- Common pattern across failures:
 - Signals **within tolerance** → no escalation
 - Issues **visible locally**, invisible at enterprise level
 - Humans **in-the-loop in theory**, not effective in practice
 - Controls designed for:
 - Static models
 - Human decision speed
 - Clear functional boundaries

WhitePine Financial: AI as a Cross-Cutting Risk

Discussion: If you were the CRO, what actually failed?

1. Detection:

- What should have triggered escalation earlier?
- What signals matter beyond model performance?

2. Governance:

- Where does end-to-end accountability sit?
- Why did “everyone did their job” still fail?

3. Control:

- Why did human override fail in practice?
- What does this imply for agentic AI governance?

Key Questions:

1. Is this a failure of controls — or of the overall risk architecture?
2. Who in this organization actually owns the outcome of AI decisions?

WhitePine Financial: AI as a Cross-Cutting Risk

Takeaways: What This Case Reveals About AI Risk

- 1. Risk shifts from model performance → system outcomes**
 - “Model working as designed” ≠ acceptable outcomes
- 2. Governance must operate at system level**
 - Not model / business / compliance in isolation
 - Requires **integration across lines of defense**
- 3. Human oversight must be designed, not assumed**
 - Overrides, escalation, authority must work at AI speed
- 4. AI risk is increasingly uninsurable**
 - Markets are signaling limits to risk transfer

Bottom Line:

AI is not just a new risk category, it challenges the foundation of ERM frameworks

Lunch



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: **Three Lines of Defence**

David Downie, Executive in Residence, GRI

June 2, 2026

Traditional View – Organizational Model

BCBS 328 – released in 2015

- Specific guidance on corporate and risk governance for banking organizations
- Three lines of defence model spelled out as follows:
 - First Line = The business lines
 - Second Line = Risk and compliance functions independent from the first line
 - Third Line = Internal audit function independent of the first and second line

Roles and responsibilities are clearly laid out

- First line owns and manages risk
- Second line provides independent challenge, provides standards and aggregates risks
- Third Line provides assurance

Traditional View - Issues

Second line was recognized to have some natural conflicts within this functional view

- Risk model development and validation
- Operational risk in second line activities

Some functions had both first and second-line activities

- Finance
- HR
- Technology

This led to a more nuanced view of the 3LOD as an *activity-based model*

Activity Based 3LOD

Now the more accepted paradigm

Make roles and responsibilities clear

- 1LOD activities must have a clear owner and challenger in the 2LOD while 3LOD provides assurance on completeness and effectiveness

Breaks the notion that revenue generation is the sole driver of 1LOD

What does not change is that the 2LOD is independent of the 1LOD and the 3LOD is independent of 1LOD and 2LOD

Does not eliminate conflicts but does highlight them and require special handling

1LOD Activities - Controls

- Now explicitly includes the control environment, as well as direct risk taking
- Identification and operation of controls
 - Process controls – payment systems, IT user access, credit approvals...
 - Data controls – data integrity, data manipulation checks, reconciliation
- Documentation
- Testing
 - Sometimes done in 2LOD

1LOD Responsibilities – Risk taking

- Identification of key and emerging risks
- Quantification of risk consistent with enterprise standards
- Measure, monitor and control risks within BU-level risk appetite
- Appropriate governance over risk taking
- Interface and dialogue with 2LOD on risk posture, trends, and the business environment

Do you have a head of Risk for business lines?

1LOD RCSA

- Owned and performed by 1LOD
- Process Mapping
 - Is this by business unit only or also include key processes that cut across business units?
- Identify and quantify control gaps and key risks (inherent risk)
- Map key controls to process and assess effectiveness of control (residual risk)
- Outputs include
 - Identification of issues and plan for remediation
 - Development or refinement of KRI for reporting
 - Reporting at BU levels and input into enterprise reporting

2LOD Activities

- Effective review and challenge of 1LOD activities
- Design and recommend/approve of frameworks, standards, policies to enable the effective governance of risk
- Aggregate and report on enterprise risk-taking – review against approved risk appetite

2LOD Review and Challenge

BIS view is that effective challenge is an outcome from an independent risk function working within a strong governance framework

- US Office of the Comptroller of the Currency is more prescriptive and wants challenge documented. “If it isn’t written down, it never happened.”

Areas of challenge

- Risk-taking decisions – lending/trading decisions; accumulations/concentrations of risk
- Models (broadly defined) including construction and parameterization/calibration
- Effectiveness of controls
- Conduct handling (Independent Risk Management/HR/Law)

Effective Challenge

Credible: comes from a person or team that understands the business and understands the risk profile and risk appetite of the institution

Clearly articulated: data or analysis driven

Actionable: has a tangible associated action or outcome

Case: Grand River Valley Bank

Review the case provided and at your table discuss the following:

1. What are the key issues in their proposal that you should challenge?
2. Rank them in terms of importance

Your team has crunched an enormous amount of data and conclude that this business proposal would have a significantly negative impact upon credit KRIs for Commercial and GRVB as a whole

1. Is there anything you should do before the meeting?
2. What path forward would you suggest?

Navigating Conflicts in 3LOD Activities

- There is rarely a clean implementation of the 3LOD
- Independence of 2nd and 3rd lines is most often a result of a power/influence imbalance skewed towards revenue generation
- The usual course of action is to identify the conflict and resolve or accept with compensating controls
- Not conflicts of interest in a legal sense, but rather “poacher-gamekeeper” types
- Examples
 - The CRO reports functionally to the CEO
 - The modeling team for risk and model validation both report to the CRO
 - Audit QA/QC ultimately reports to the head of Internal Audit

CEO/CRO Dynamic

- This was addressed in BCBS 328 and earlier and also exists for Chief Audit Executive
- CRO reporting relationship
 - Administratively to CEO
 - Functionally to Board Risk Committee
- CRO must have access to Board Risk Committee in order to escalate issues
- Board Risk Committee must ensure that the independent risk functions are adequately staffed and resourced
- Hiring and removal of CRO requires consent of the Risk Committee
 - Regulator is advised (Canada, US, ECB) or must approve (UK PRA)

Risk Model Development/Model Validation

Regardless of where these activities reside in the risk function, they ultimately report to the CRO

Some alternatives

- Ensure reporting for each is to two different leaders in the risk function or have model validation report to the CRO
 - Reduces the problem but doesn't eliminate it
- Move the model development outside of the risk function
 - Will require assurances that risk model development is sufficiently prioritized
 - Probably would involve transfer pricing
- Leave at the discretion of senior risk leaders to manage
 - Self-identify as a weakness in controls and governance
 - Audit would review outcomes

Audit QA/QC

- Chief Audit Executive, or report would have QA/QC report to them
- Outsourcing of entire function is probably not viable or practical

Some approaches to resolve:

- Hire an external party to review QA/QC on a regular basis
- Acknowledge control and governance weakness and provide transparency to audit committee



**GLOBAL
RISK**
INSTITUTE

Emerging Leaders Program: **Risk Culture**

David Downie, Executive in Residence, GRI

June 2, 2026

Risk Culture

Best thought of as an outcome, not an objective/destination

- the “how” that facilitates the “what’ in the risk governance ecosystem
- Good Culture = Robust governance infrastructure (frameworks, policies, limits) X strong behaviours

Poor culture can undermine governance even when processes and infrastructure are strong and comprehensive

- Behaviors must be constantly reinforced by all levels of the organization

Nebulous by nature

- No uniform definition of “risk culture” or “culture risk”
- Most often exposed or evaluated in retrospect

Foundations

Clarity on roles and responsibilities

- Especially 1LOD risk vs 2LOD

Robust governance and control environment

- Including frameworks, policies and compensation practices
- Well-understood risk taxonomy

Tone from top and middle

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

- Credible consequences for actions deemed detrimental to culture

Culture Governance (OSFI 2024)

The **Board** is responsible for the institution's culture

- “should promote a risk culture that stresses integrity and effective risk management”

Senior Management is responsible for culture risk management must

- set the tone for the desired culture
- put in place
 - Talent and performance management tools and processes to reinforce the desired culture
 - Appropriate compensation, rewards and recognition systems
- proactively manage culture
- embed culture risk into the ERM framework

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

Some 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

Supervisory Approaches

Fundamentally an issue of moral hazard, or “hidden action”

- No CEO nor CRO will admit that their culture is poor
- FRB: try to force banks to “unhide actions” by documenting every material risk decision and the challenge provided
- FCA: financial and possible criminal penalties for outcomes that are tied back to culture
- OSFI: more prudential approach – integrated in all aspects of the institution and examined in that manner

All major regulators understand the role of culture and the difficulty to develop, measure and maintain

Metrics and Reporting

Typical measures

- Overdue training, complaints, whistleblowing
- Limit breaches and conduct issues
- Loss event reviews

Newer tools

- Surveillance of e-mails, chats, committee minutes
- Inferences drawn from decision flows (approvals, escalations, over-rides)

Mapping these into a model and calibration remain a challenge

Networking Reception

Don't forget to complete the survey