Dealing with Operational Resilience in TPRM

Learning from the Titanic

Vrushali Lakhpati

Vice President,
Third Party Due Diligence Program
AmTrust Financial Services

Agenda

- About Operational Resilience
- Overview of Titanic tragedy
- Applying lessons from Titanic
- Keys to success
- Final takeaways

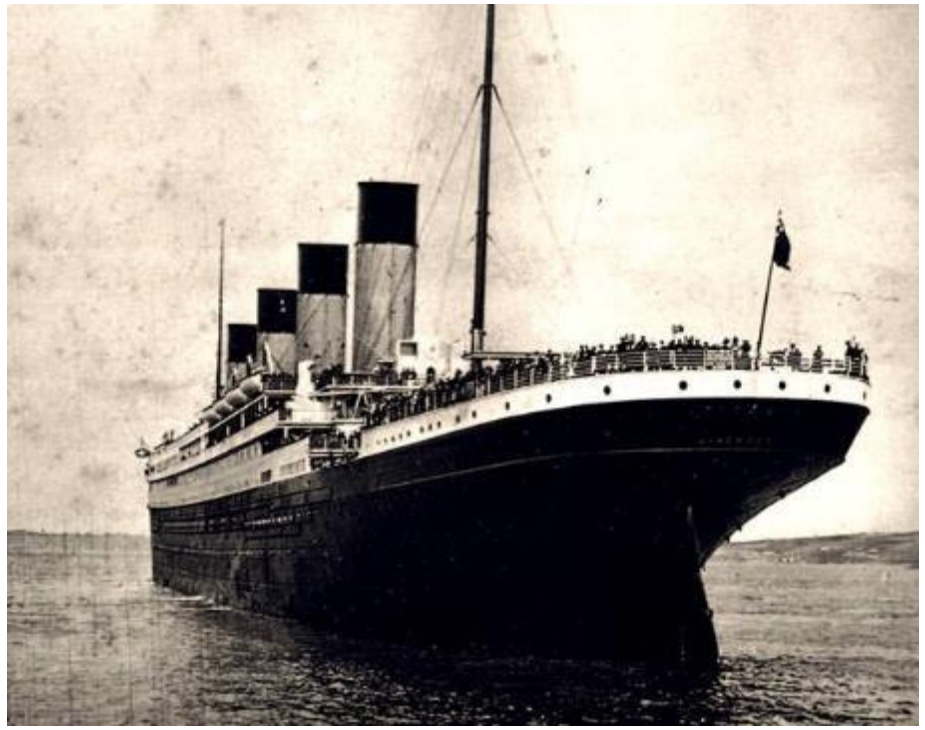
What is Operational Resiliency?

The ability of an organization to prevent, withstand, and recover from operational disruptions, whether caused by internal or external events

Operational resilience is fundamental to TPRM as it enables organizations to remain robust, sustainable and compliant to regulatory requirements when relying on extended third party enterprise

Overview of the Titanic Tragedy

Titanic: The Unsinkable



Royal Mail Steamer (RMS) Titanic

$7.5M
Building cost

2,000+
onboard

2,070
Miles sailed

Timeline

March 31, 1909	Construction Begins
May 31, 1911	Titanic Launched
Apr 10, 1912	Maiden Voyage
Apr 14,1912	Iceberg Spotted
Apr 15, 1912	Titanic Sinks

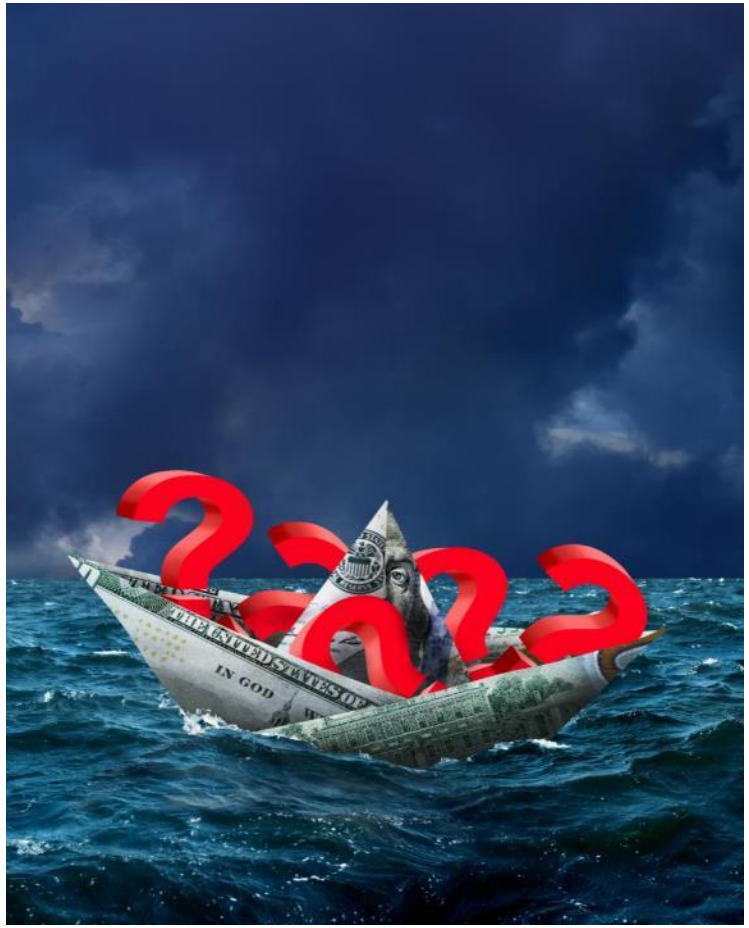
3000+
workers

3 Years
to build

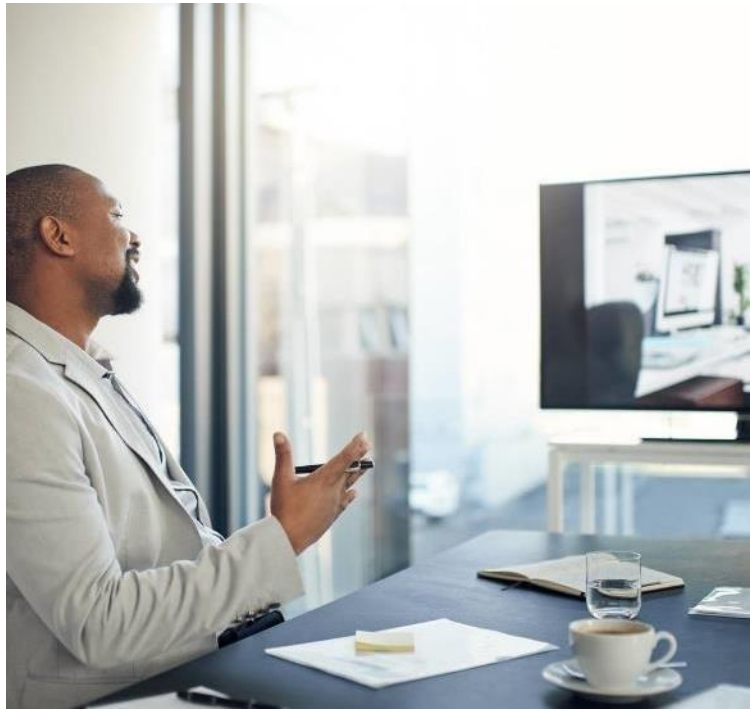
3 hrs.
to sink

1,500+
Lost lives

Key Events Leading to the Disaster



- Overconfidence in safety measures
- Ignored warning signs
- Ineffective communication
- Inadequate risk assessment
- Inadequate contingency planning
- Training deficiencies



Applying Titanic Lessons to TPRM

Insights from history for better risk management

Overconfidence in Safety Measures

The Titanic was deemed 'unsinkable' leading to false sense of security. Complacency was prioritized over safety

Comparison to TPRM:

- Executives can become overconfident in their TPRM program strategies or technologies which may blind them to real and evolving risks
- Overconfidence could manifest in ignoring warnings signs, resulting in unpreparedness in dealing with potential threats or disasters
- Organizations may misjudge resilience by investing in the best TPRM technology but fail in building a robust process including clear role and responsibilities

Ignoring Warning Signs

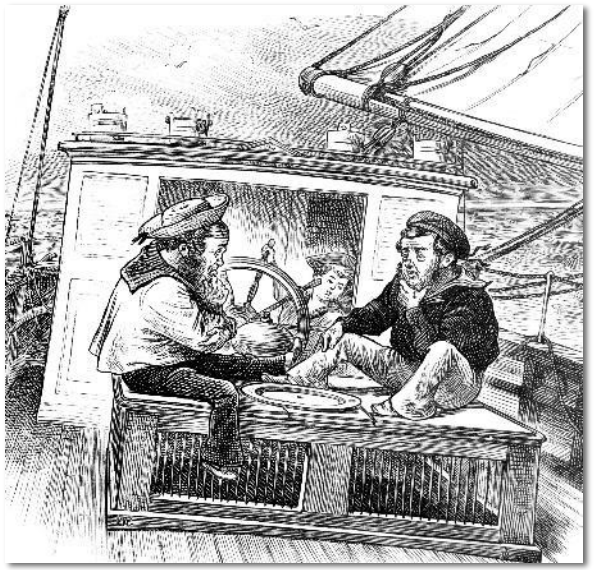
Multiple Iceberg warnings were disregarded by the crew

Comparison to TPRM:

- Early warning signs with third party relationships could be missed, such as:
  - Poor financial and credit ratings
  - Weak cybersecurity risk ratings
  - Negative news / politically exposed persons (PEP)
  - Lack of BC/DR plans
  - Recent cybersecurity incidents
  - Issues in SOC 2 Type 2 reports
  - Lack of adequate insurance coverage
- Reliance on retrospective data limits visibility into real-time operational risks

Ineffective Communication

Several iceberg warnings were received but not adequately communicated to the crew



Comparison to TPRM:

- Lack of oversight and accountability can have a significant impact in obtaining timely insights on the risk posture of the third parties
- Lack of clear communication channels may impact a prompt response during disruptions
- Clarity in communication is vital for risk mitigation and risk based decisioning
- Disparate technologies often cause problem in collating and sharing information
- Societal factors such as language may becomes a barrier in communication

Inadequate Risk Assessment

Failed to adequately assess the risks of navigating icy waters. Steel became brittle in sub zero temperature

Comparison to TPRM:

Third Party Risk assessments often:

- Are check in the box activity
- Lack access to real-time external data leading to ignorance or downplaying the risks identified
- Don’t account for controls to protect against emerging risks
- Rely on outdated and point in time assessment questionnaires
- Limit visibility into extended supply chain risks
- Do not provide holistic view of third party risks

Inadequate Contingency Planning

Lifeboat capacity and emergency response protocols were not adequately reviewed or tested

<u>Comparison to TPRM:</u>

Lack of robust contingency in managing critical/high risk third-party relationships may result in:

- Significant impact to Business operations
- Limit the ability to act promptly in crises
- Ineffective scenario testing to stimulate disruptions
- Non-compliance with tolerance levels

Weak links in the supply chain, outdated technology, or poor-quality products and lack of resources can all contribute to a larger disaster if left unaddressed.

Training Deficiencies

Lack of training left the crew unprepared for the emergency escape; lifeboats left the ship half-empty

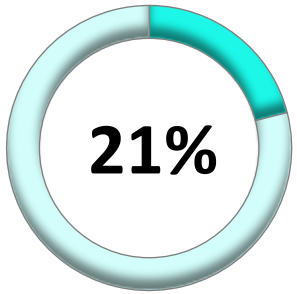
Comparison to TPRM:

- Lack of necessary TPRM skills and knowledge to interpret potential risks can derail even the best TPRM programs
- Lack of training can lead to vulnerabilities, compliance issues, and inefficiencies going undetected
- Internal and external stakeholders may not be trained on operational resilience practices
- Lack of an awareness and understanding of TPRM policies and procedures and training on tools and technology may result in in-consistency in practices

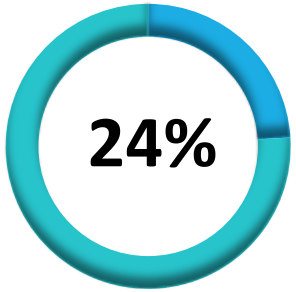
What can happen when Operational resilience within TPRM is not understood or addressed?

- **Service interruptions**
- **Financial losses**
- **Reputational damage**
- **Lack of continuity of critical operational**
- **Non-Compliance with regulatory requirements**
- **Impact to supply chain resilience**
- **Lack of stakeholder confidence**

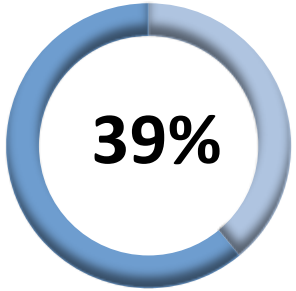
Are we addressing emerging risks in 2025?



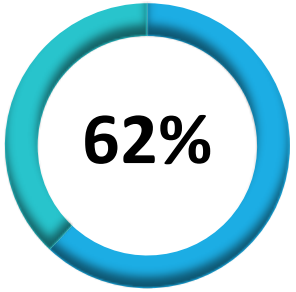
Proactively managing emerging risks



confident in the ability to prioritize emerging risks



conduct business resiliency exercises to test preparedness



business continuity plans do not adequately help the organization deal with unexpected events

Gartner Report: Emerging Risk Identification and Management Primer for 2025

The Blue Screen Of Death Due to CrowdStrike Error

Cybersecurity firm CrowdStrike caused the Blue Screen of Death (BSOD) on many Windows computers due to a faulty update to the Falcon Sensor agent

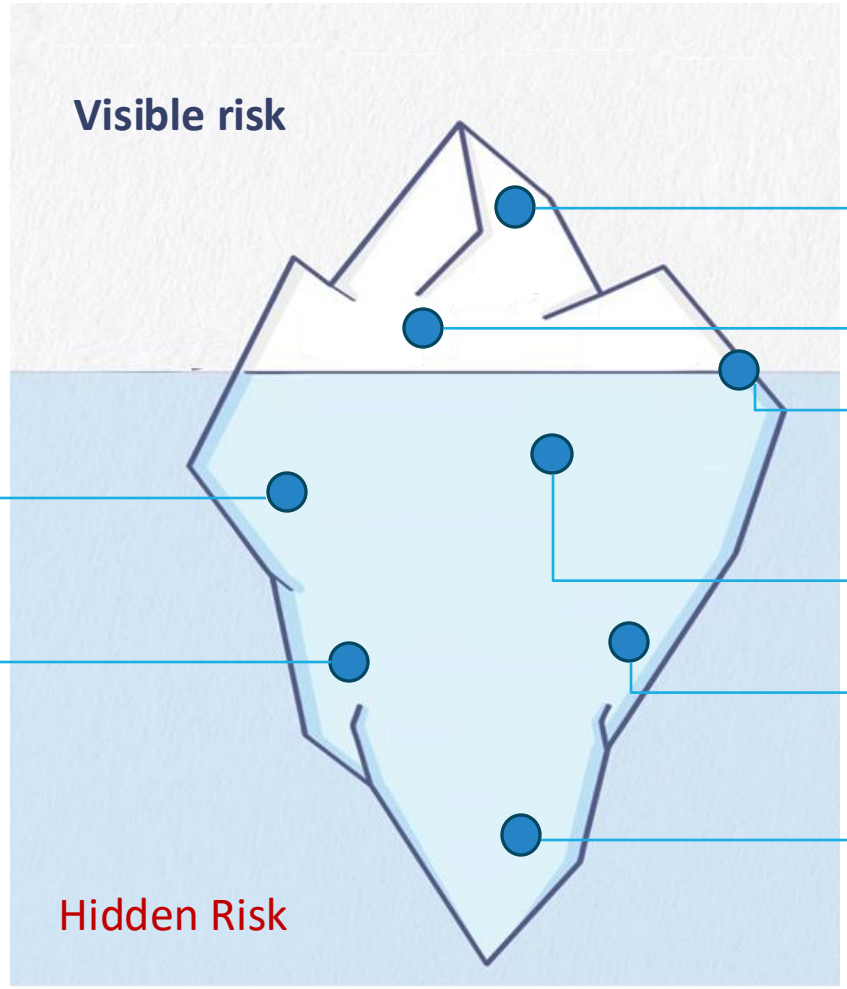
The cyber resilience alarm heard around the world

- ~8.5 million Microsoft Windows devices were affected on 19th July 2024
- Disruptions of airlines, banks, stock markets, broadcasters, healthcare providers, emergency services, gas stations, retail payment terminals, cash machines and more
- Cost of the outage is estimated to top **$1 billion**

Keys to Success


How can we implement insights from historical events to strengthen Third-Party Risk Management (TPRM) strategies and increase resilience?

Managing third-party risk during unprecedented times



Risk Assessment Practices

Regulatory Compliance

Contract Management

Contingency Planning and Collaboration

Proactive Monitoring and Mitigation Strategies

Scenario Testing and Simulation

Communication and Escalation

Training and Skill Development

Risk Assessment Practices

Conduct thorough risk assessments

- Identify critical functions and operations
- Prioritize third parties based on criticality
- Extend risk coverage across enterprise risk domains
- Leverage internal and external data
- Account for recent disruptive changes in the third-party risk posture

Evaluate operational practices

- Assess business continuity and disaster recovery plans
- Check third parties' ability to handle disruptions
- Identify critical or important business functions and map critical services

Choose vendors with strong resilience

- Select vendors with robust operational resilience capabilities

Regulatory Compliance

There has been a global regulatory focus on maturing operational resilience to enhance focus on critical functions and business services supported by third parties.

Global Regulatory Key Themes

- Governance and accountability
- Due Diligence Practices
- Risk-based approach to identify critical third parties
- Criticality of data & comprehensive inventory
- Fourth Parties & Concentration Risk
- Contingency & Exit Planning
- Contract Management

Examples include:

- Digital Operational Resilience Act (DORA)
- Prudential Regulation Authority (PRA)
- Financial Conduct Authority (FCA)PS21/3
- Central Bank of Ireland (CBI)
- International Organization of Securities Commissions (IOSCO)

Contractual Management

Resilience-focused language in contractual agreements including:

- Business Continuity Planning and testing
- Termination clauses
- Sub-contracting requirements
- Rights to monitor performance on an ongoing basis
- Right to inspect and audit
- Response times expectations
- Communication guidelines and protocols
- Reporting requirements

Contingency Planning and Collaboration

Collaborate with vendors

- Define overall risk appetite and tolerance for disruption
- Develop joint contingency plans for various disruption scenarios
- Align of recovery time objectives (RTOs)
- Identify fourth parties and potential disruption and unavailability

Outline roles and responsibilities

- Clearly define roles and responsibilities
- Establish communication strategies

Ensure leadership commitment

- Foster a culture of resilience and secure the resources needed to implement effective strategies

Scenario Testing and Simulation

Conduct Regular Scenario Testing

Simulate disruptions involving third-party vendors

- Desktop Scenario exercise
- Simulated, stressed scenarios exercise
- Live test
- Incident scenario

Evaluate Management and Recovery

- Assess how well both parties manage and recover from scenarios

Identify Areas for Improvement

- Adjust contingency plans based on findings

Communication and Escalation

Establish Clear Communication Channels

- Establish regular communication protocols with employees, stakeholders, clients, and regulators
- Establish feedback loop with third parties to address issues

Quick and Coordinated Responses

- Develop RACI frameworks and escalations during incident and crisis management
- Proactively communicate potential threats and issues
- Respond promptly during disruptions

Develop a reporting framework

- Share periodic reports to key stakeholders based on Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs)
- Increase frequency of communication for critical suppliers

Proactive Monitoring and Mitigation Strategies

Perform ongoing risk assessments including:

- Inherent risks & third-party due diligence
- Third party performance / SLAs
- 4th party and supply chain risks

Monitor and report early warning signs

- Drop in cybersecurity ratings
- Change in employee turnover
- Working capital ratio
- Trends of critical outages

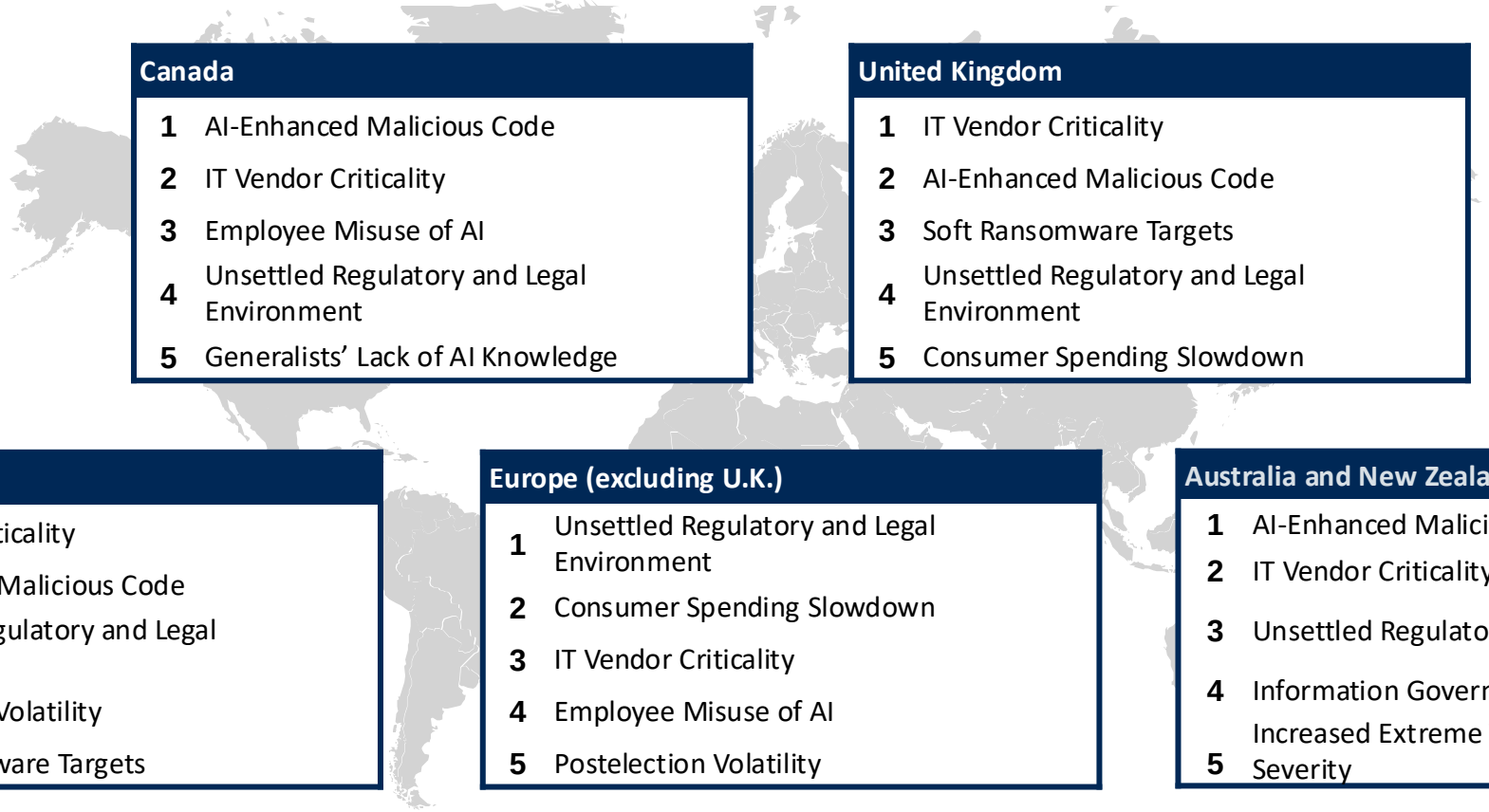
Perform Business Impact Analysis to assess risk interdependencies

- Concentration risk impacts
- Operational and business continuity impacts
- Reputational damage
- Regulatory exposure

- Review exit strategies for critical service providers
- Monitor regulatory updates or new government laws / policies
- Monitor global events

4Q4 Gartner Emerging Risks Report

Top Five Emerging Risks
By Risk Score



Canada

1	AI-Enhanced Malicious Code
2	IT Vendor Criticality
3	Employee Misuse of AI
4	Unsettled Regulatory and Legal Environment
5	Generalists' Lack of AI Knowledge

United Kingdom

1	IT Vendor Criticality
2	AI-Enhanced Malicious Code
3	Soft Ransomware Targets
4	Unsettled Regulatory and Legal Environment
5	Consumer Spending Slowdown

United States

1	IT Vendor Criticality
2	AI-Enhanced Malicious Code
3	Unsettled Regulatory and Legal Environment
4	Postelection Volatility
5	Soft Ransomware Targets

Europe (excluding U.K.)

1	Unsettled Regulatory and Legal Environment
2	Consumer Spending Slowdown
3	IT Vendor Criticality
4	Employee Misuse of AI
5	Postelection Volatility

Australia and New Zealand

1	AI-Enhanced Malicious Code
2	IT Vendor Criticality
3	Unsettled Regulatory and Legal Environment
4	Information Governance-Driven AI Risks
5	Increased Extreme Weather Frequency and Severity

n = 10 (Canada); 133 (United States); 14 (United Kingdom); 18 (Europe, excl. U.K.); 19 (Australia and New Zealand).
Note: Mexico, Central America/South America, Middle East, Africa, and Asia/Pacific (excl. Australia and New Zealand) are not presented due to n size.

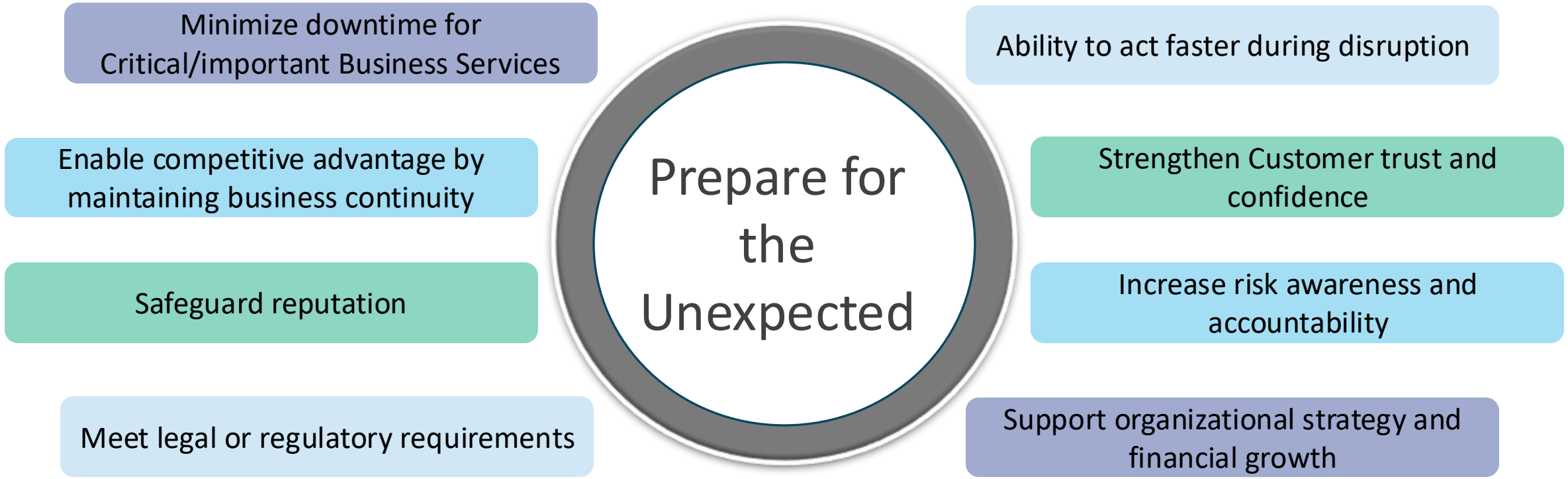
Risk Score = Cube Root (Impact x Inverse Time Frame x Frequency Selected as a Top 10 Emerging Risk Rescaled)

Source: 4Q24 Gartner Emerging Risks Report Survey, n = 208

Training and Skill Development

- Educate employees and provide ongoing trainings
- Promote a security-conscious culture
- Ensure awareness on roles and responsibilities in managing disruptions
- Leverage automation to reduce reliance on manual processes
- Empower teams to respond effectively to disasters and mitigate risks
- Share lessons learnt from incidents or challenges
- Enhance your professional credibility with online TPRM knowledge resources or certifications like Third Party Cyber Risk Assessor (TPCRA)

Why should you strengthen Operational Resilience in your TPRM program?



Thank you