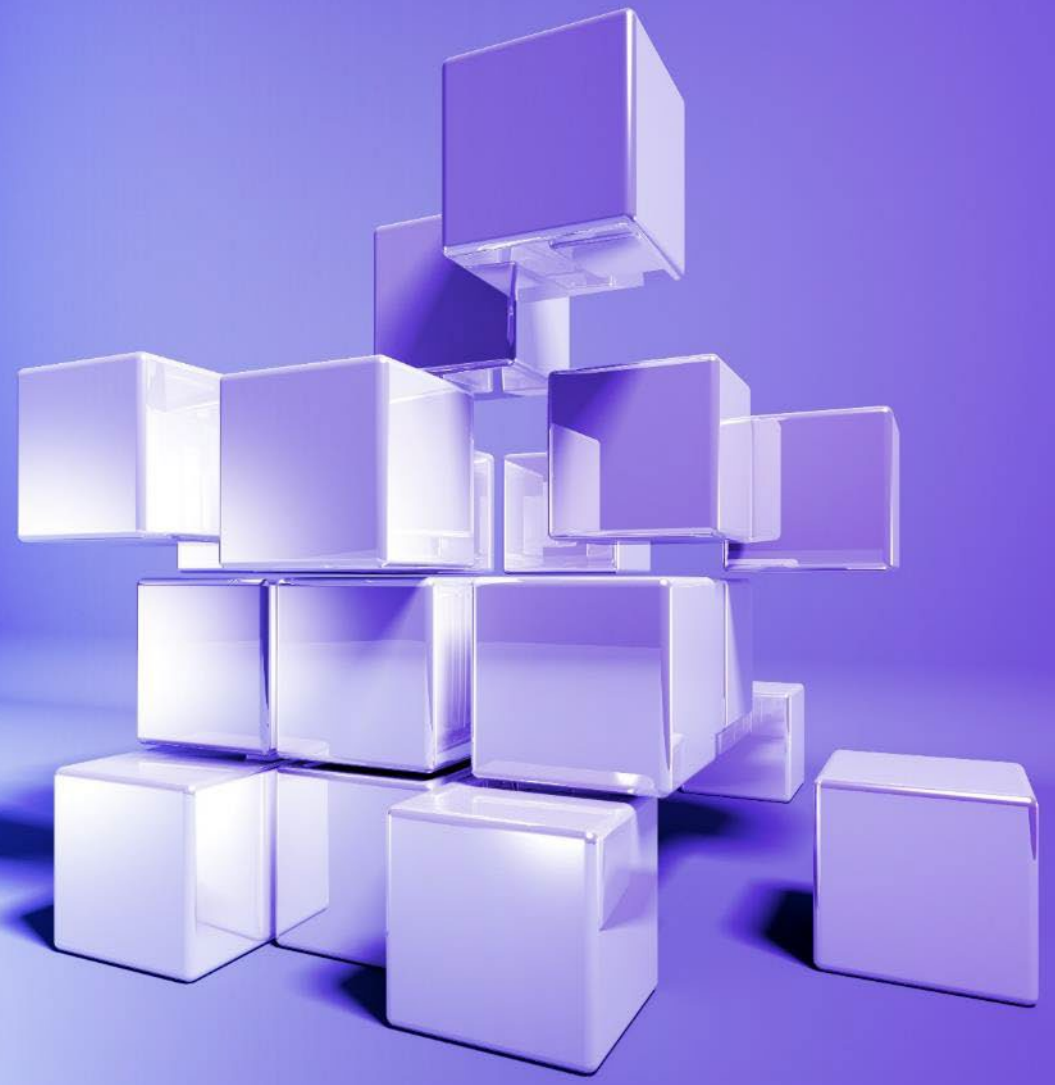
KPMG

Risk Intelligence and Quantification

Utilizing technology and automation to manage risk assessment and monitoring



IIA Atlanta

June 2023

Content

01

Evolution of Risk Assessment and Monitoring

Scanning the horizon

Advancing the use of data and digitization to address challenges and prepare for the future

- Aggregated view of risk
- Enhanced data driven insights
- Integrated risk assessment process
- Valuable risk led insights
- Adapting to the changing landscape
- Real time risk indicators
- External risk insights
- Proactive monitoring

We are surrounded by data, but starved for insights – Jay Baer
marketing and customer experience expert

Data is everywhere, it is up to us to make it meaningful, One study found that businesses are missing out on $5.2M in revenue due to untapped data. The data exists but not everyone is using it, nor do they know how to get the value.

KPMG's approach to data-driven risk assessment uses a thoughtful methodology supported by analytics and visualizations. This is to increase efficiency, enable evidence-based decision-making, and deliver valuable insights.

The future Chief Audit Executive (CAE) agenda

Leading organizations have developed an agenda to help deal with disruption across their internal audit functions

Focus areas for today

Stakeholder engagement and trust

Internal audit knows its top stakeholders and takes the time to foster a relationship of trust attuned to their needs

Digital acceleration

Leverage technology with organizational goals in mind, and use it to enable program and project level work

Data, analytics and insights

Enterprise data is available and used, and new data is curated by internal audit. This data is used to provide risk insights and enhanced assurance through broader audit coverage

Strategy and value management

Internal audit strategy considers a mix of enhanced assurance, risk insights and business improvements attuned to stakeholder needs. Strategically important and future-focused emerging risks are prioritized

New ways of working

Where services are delivered, the competencies that enable that delivery, and the way audit teams want to work has to be revisited to help retain the right talent

Operating model agility

Audit activities are responsive to disruption, flex with the business strategy throughout the year, and consider coordination with other lines of defense

Stakeholder engagement and trust

Internal audit (IA) knows its top stakeholders and takes the time to foster a relationship of trust attuned to their needs

Know your stakeholders

Internal audit knows its top stakeholders and invests the time needed to foster a relationship of trust attuned to their needs

- Internal stakeholders are IA's top priority, particularly the Board / AC and select executives and front office leaders
- IA supports these internal stakeholders and associates with second line functions to help the organization better meet its obligations to external stakeholders
- Relationships of trust are built through demonstrating IA's relevance; critical attributes of a trusted relationship are empathy, logic, and authenticity

Be a strategic advisor

Through having a relationship of trust, internal audit is included in high-level value-add conversations as a strategic risk advisor or problem solver

- IA routinely probes its internal stakeholders on arising initiatives and changes in their business
- As IA becomes aware of these initiatives, they serve as an advisor by participating in planning discussions and assessing the potential benefits of changing its plan as needed to provide consultative support or real-time assurance

Commit resources

To adequately act as a strategic risk advisor or problem solver, internal audit makes the resource commitment to address ad-hoc requests by the business

- The audit plan has built-in flexibility to take on project work for these ad-hoc requests
- Metrics around involvement in change initiatives, ad-hoc requests and points of impact (i.e. improvements implemented as a result of audit work) are monitored as KPIs

KPMG

Key Client Pain Points

Internal Audit organizations are grappling with the same rapid technology and digital acceleration challenges as the rest of the organization, but with the added need to:

- **Be proactive vs. reactive**
- **Keep pace with internal drivers of change**
- **Produce deeper, actionable insights on risk**
- **Address shifting regulations, social expectations and cultural understanding**

In order to meet the evolving stakeholder needs of the organization, IA functions need to tackle root causes of inefficiency, including:

Ad-Hoc Reporting

Inability to process data and create reports in a timely and standardized manner, resulting in delays with executive information sharing and remediation.

Opaque Monitoring & Remediation Processes

Minimal visibility into assets non-compliance and prolonged remediation lifecycles due to manual processes.

Inadequate Metrics

Non-existent or ill-defined metrics, hampering the organization's ability to monitor compliance against company standards.

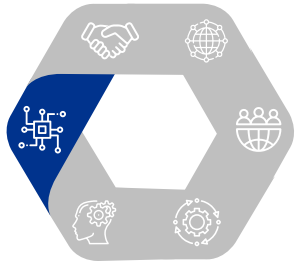
Disparate Data Sources & Systems

Lack of a unified data repository to centralize and combine siloed data source.

Digital acceleration

“For a majority of U.S. CEOs, the pandemic has meant an acceleration in digital transformation by months or even years. The move to digitization has accelerated and the potential benefits are expected to be permanent. There is no going back.”

– Carl Carande, Vice Chair for Advisory at KPMG in the US.

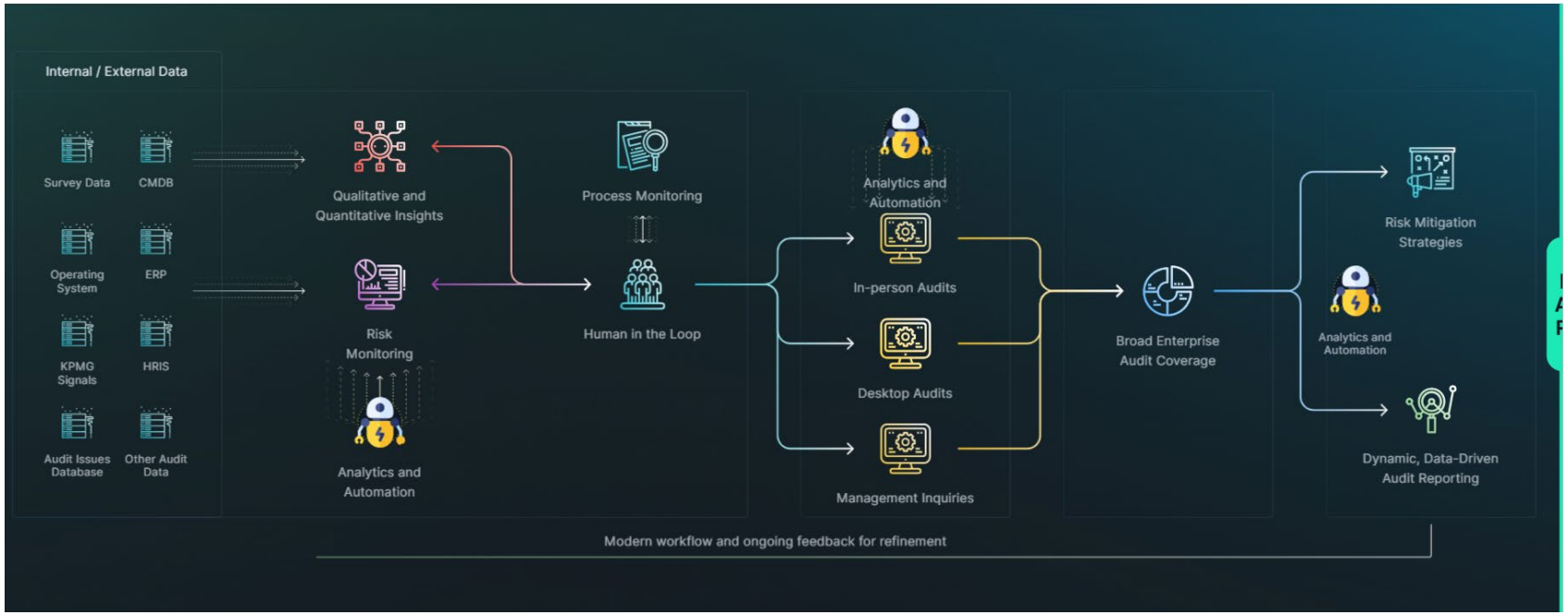


Strive to thrive amid disruption

Internal audit technology is selected with organizational goals in mind to provide as much integration and synergy as possible

Audit work is enabled via automation and technology at program and project levels

Internal audit supports business objectives for digital acceleration through AI controls and assurance over digital initiatives and transformation



A glimpse into KPMG firms' digital internal audit story

The Future of Internal Audit Story

ADD KPMG INSIGHTS CENTER STORIES

Future of IA

Insight Center Access (wisewindow.com)

Data, analytics, and insights

Use of data analytics continues to be a powerful tool for the internal audit function to help assess risk and provide insights to assist management decision-making on process improvements and control effectiveness.

Assessment and Monitoring

Testing and Execution

Advanced Risk Analytics

Risk Sensing
process patterns, detect anomalies.

Risk Scoring
quantify likelihoods and impacts for comparison.

Risk Reporting
visualize insights, considers scenarios

Metrics
packages of measures and indicators.

Modern Data Platform

Connectors
retrieve data from core systems

Marketplace
space for users to explore and share

Standards
align data to consistent framework

Enable teams to embed analytics that improve monitoring and drive insight and consistency into mitigation and reporting activities.

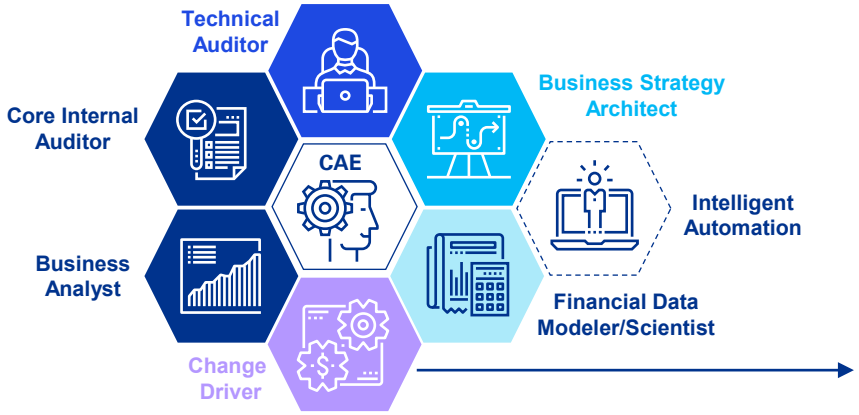
- Focus on value and measure the success of every analytic;
- Use the tools at hand, deploy to any cloud and most platforms;
- Engage owners, ensure smooth transitions and provide reach-back support.

KPMG

New ways of working

Where services are delivered, the competencies that enable that delivery, and the way audit teams want to work should be revisited to retain the right talent.

Critical talent base and skillset considerations



To move into a more strategic, advisory role to management, alongside its assurance objectives, internal audit departments are adapting the profile of the typical candidate they hire into internal audit.

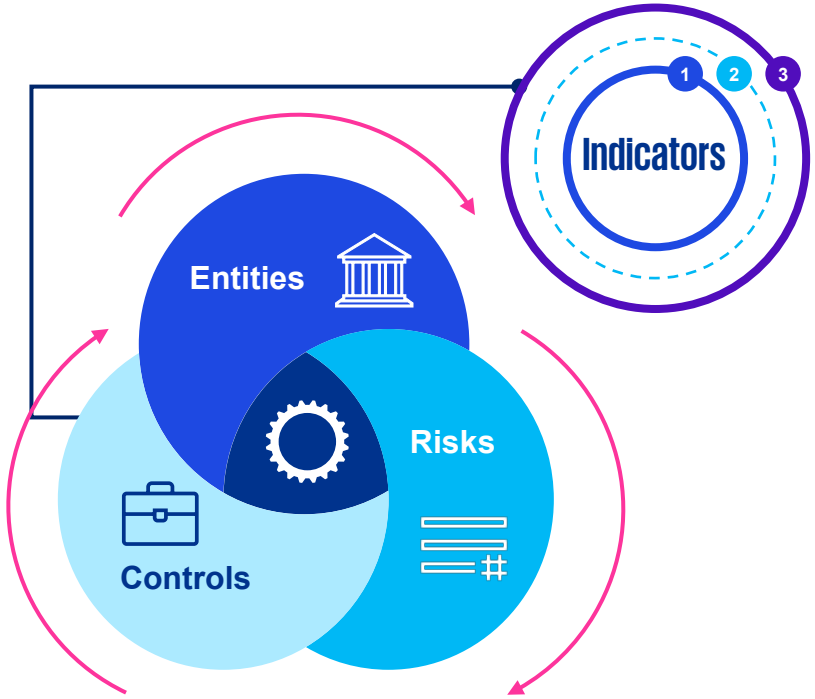
Hiring profiles will likely include a mix of strategic, behavioral and data utilization and technology skills alongside internal audit technical skills.

- Critical thinking and problem-solving skillsets, including enterprise acumen and cultural and behavioral awareness, take priority over expected core audit skillsets
- Proficiency around technology and analytics are assumed to be within core audit skillsets through increased investment in a data-driven approach
- Re-skilling existing team members, bringing in new and temporary auditors, and adjusting to remote working are key enablers
- Tasks are performed through a mix of automation, rotational employees, temporary employees, subject matter professionals, core team members, strategic sourcing, and offshore / nearshore capabilities
- A change driver becomes a critical role for driving value and overall business performance.

KPMG

Analytical Process for Risk Rating & Quantification

Leveraging a defined data-driven and analytical process allows you to standardize indicators to generate quantified risk ratings for risk professionals to manage / mitigate co-employment risks.



Quantification engine uses indicators to score the severity of **risks**, effectiveness of **controls**, and exposure of business **entities**. These enterprise elements are arranged hierarchically enabling aggregation and drill-down.

1 Features

Standardize risk indicators to thresholds and tolerances. Calculate distance, velocity, persistence.

2 Probabilities

Define conditional relationships between indicators and enterprise elements. Specify likelihood ranges.

3 Risk Factors

Fit magnitude and direction of relationship between indicators and elements. Potential use ML or AI to better inform/update risk factors.

Dashboards

Discover risk ratings across hierarchies and over time.

Recommendations

Consider preferred mitigation options, compare scenarios.

Graphs (Networks)

Explore mappings and relationships that propagate risk through enterprise.

KPMG

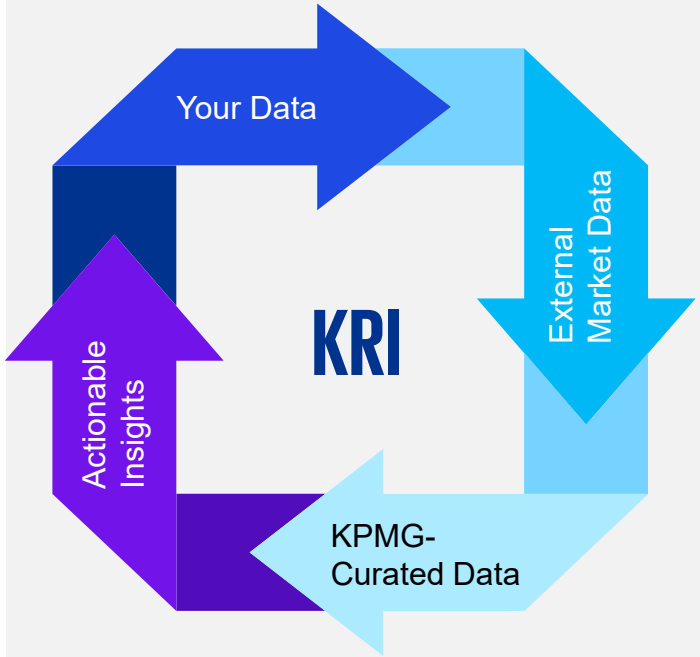
KPMG's answer

Digital platform that aligns an organization's lifecycle of risk decision making, with optimization in mind

Leverages KPMG's leading Risk Services knowledge to provide curated data in support of comprehensive risk assessment and monitoring

Delivers insights for C-suite, Board members, and risk consumers to help demystify risk return

KPMG Risk Intelligence (KRI) provides insights to help an organization answer:



- Where is the greatest possibility of disruption?
- What is the exposure (e.g. does our company / business unit have risk to country / location)?
- How can we better look ahead?
- What risks do we need to prioritize?
- How can we use internal and external data to make better decisions?
- What is the risk-return trade-off for an action?
- How do I compare to my peers?

KPMG Risk Intelligence capabilities

Our platform is built within the Microsoft Azure cloud, with additional survey and visualization tools leveraged for user interface and reporting capabilities.

The solution provides three sets of capabilities through modules, which can be selected in part or whole to meet each organization's needs.

Assessment

Automates risk assessment processes and reporting

- Customizable taxonomies
- Configurable surveys and features
- Risk Analysis Review Results
- Interactive Risk Analysis Reporting

Monitoring

Ingests internal, external, and KPMG-curated data to provide real-time monitoring and reporting

- Interactive Risk Monitoring/ Trending Reporting
- Risk Appetite and Tolerance
- External Risk Metric Insights
- Internal Risk Metric Portfolio
- ESG & Signals Repository

Intelligence

Enhanced ability to connect multiple data sets to provide comparisons and assign dollar values to identified risks

- Risk Dollar Quantification
- Automated Insights
- ERA / SRA
- Peer Comparisons Powered by Benchmarking+

Demo of KPMG Risk Intelligence

https://vimeo.com/833428657/737fd4b445?share=copy

03

Leveraging analytics to drive value: *Use Cases*

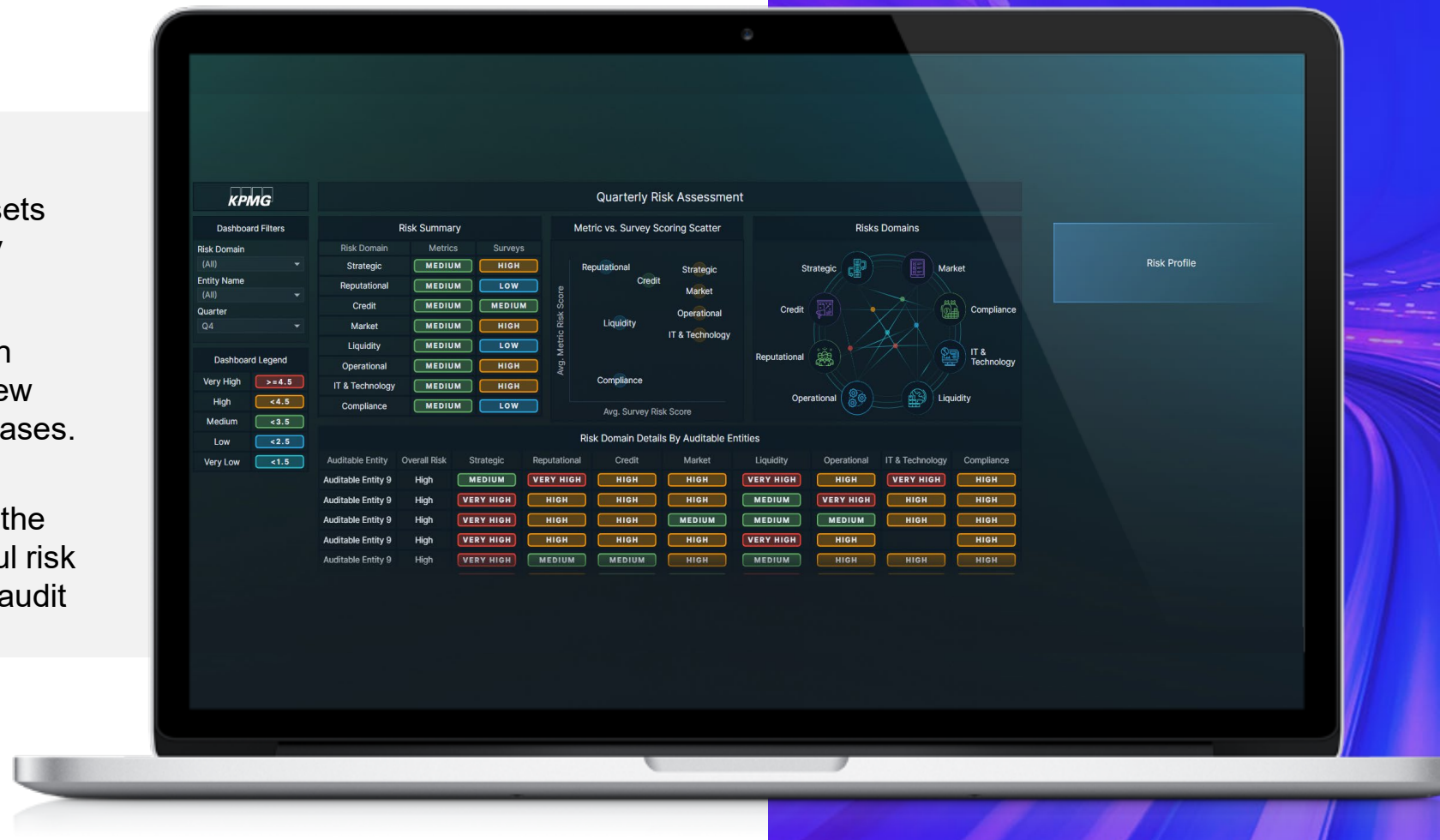
USE CASE #1

Prototype of dashboard reporting

KPMG Risk Intelligence can ingest a variety of internal and external data sets to serve as risk indicators across any population and risk categories.

These data-based risk indicators then provide a data-enabled risk profile view that can be used in a variety of use cases.

Using Risk Intelligence for a heterogeneous set of entities across the organization enables a more insightful risk profile to monitor risk and inform the audit plan.



USE CASE #2

Extensive internal quantitative metrics

Scenario

An organization used risk monitoring to better assess and monitor part of their business operations leveraging 85 internal quantitative metrics.

Tools used

USE CASE #3

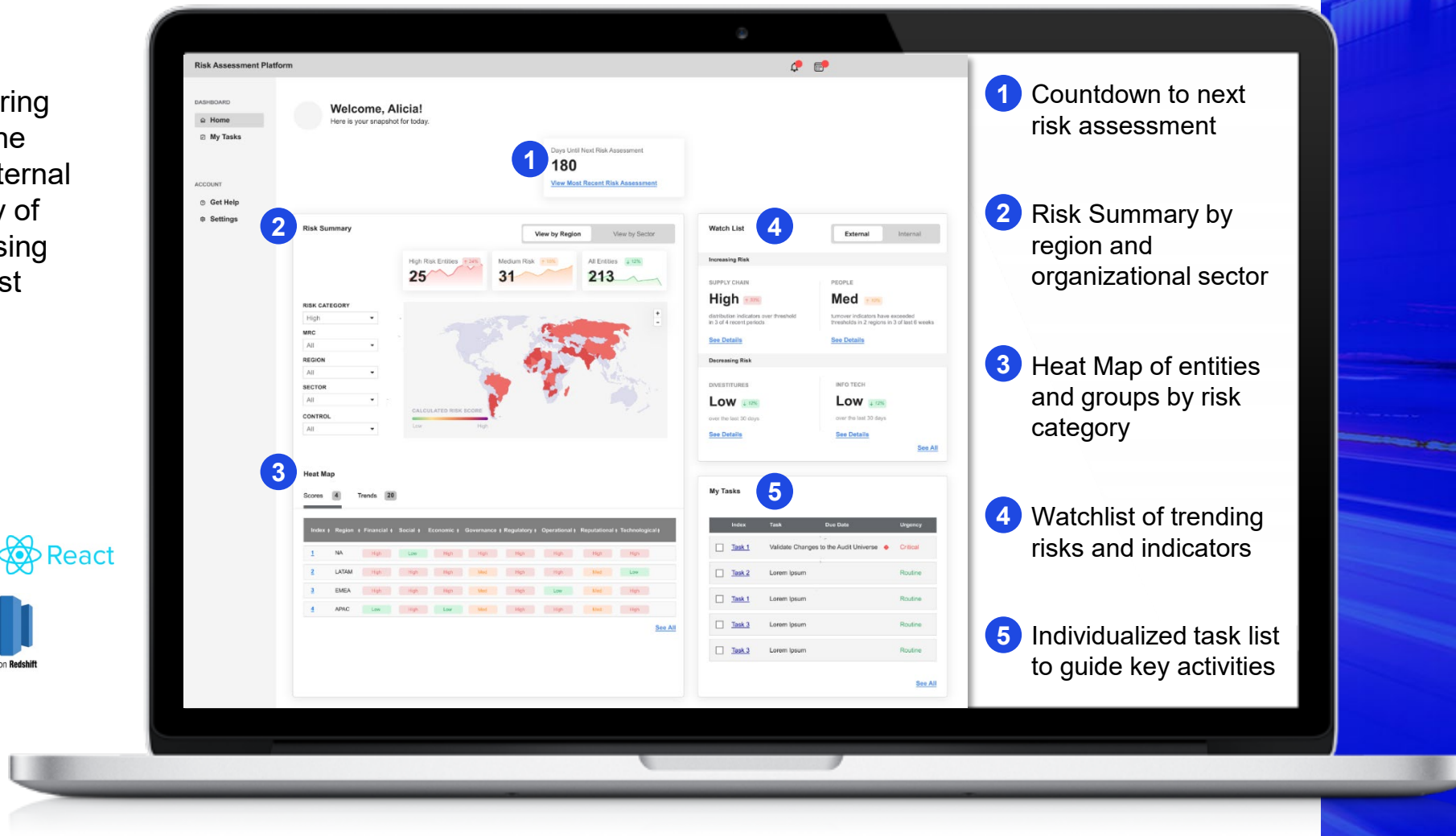
Extensive quantitative and qualitative metrics

Scenario

An organization used risk monitoring to better assess and determine the locations for their international internal audit activities based on a variety of internal data points – better focusing resources on areas of the greatest risk.

Tools used

MuleSoft, alteryx, Amazon S3, neo4j, LINKURIOUS VISUALIZE GRAPH DATA EASILY, python, +ableau, React, AWS Amplify, PowerApps, amazon RDS, Amazon Redshift



04

How to Get Started

Considerations on the data journey

Considerations

Availability

Is the data readily available for the audited process? Does Audit have access to all necessary data sources? Consistent API's or single source?

- Comprehensive understanding of data
- Data exists and fully available / accessible

Data Quality

Is the data being captured in a consistent nature and complete? Is it in a structured, relational database or unstructured in a data lake?

- Structured / unstructured
- Reliability of data and relationships

Risk Impact

Does the audited process/area represent a high concentration of risk and impact to the organization?

- Risk taxonomies
- Metrics

Complexity

Is the data being obtained from multiple source systems? Is the time required to obtain and validate the data low?

- Multiple Systems / High Effort
- One System / Low Effort

Repeatability

Will the audit be performed multiple times using a similar data source (e.g., same ERP or quarterly audit)?

- Ad Hoc
- Continuous Risk Assessment / Continuous Auditing / Continuous Monitoring / Full population testing

How to Get Started

People

What works:

- Hiring specialists: 2-3 or 10% of the department
- Building a Center of Excellence
- Partnering with a team of SMP's to build out the capability
- Borrowing/Rotation D&A resources internally or externally

Less successful approaches:

- Training everyone
- Training a few
- Everyone will do analytics
- Including D&A in their goals
- Allocating a percentage of a few people's time

Process

What works:

- Analytics in risk assessment
- Using analytics in scoping
- Using analytics in testing
- Dashboard reporting
- Using analytics to find problems
- Using analytics to help solve problems

Less successful approaches:

- Requiring analytics in all phases
- Requiring exception form be signed by CAE to not use analytics
- Continuous Auditing Projects in silos
- More Analytics = More Value (Run it ALL!)

Technology

What works:

- Using enterprise analytics tools
- Using visualization tools (Tableau / PowerBI)
- Building an IA data warehouse
- Direct database access

Less successful approaches:

- Buying audit-centric tools
- Buying technology as the first step in implementing a DA strategy
- Requesting custom reports from IT

KPMG

Dynamic Risk Assessment (DRA)

Discussion with the IIA

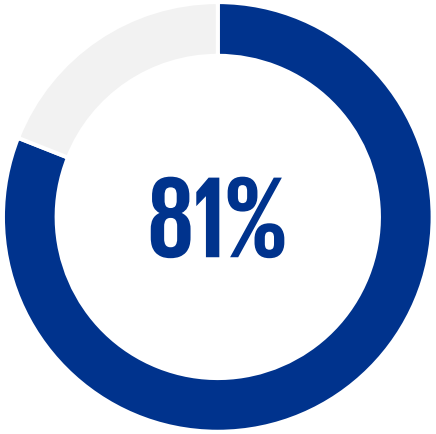
Preparing for the unprecedented in an interconnected world

June 2023

Preparing for the future with Enterprise Risk Management

It's not enough to know what's happening if you didn't see it coming

- Big data
- Artificial intelligence
- Supply chain challenges
- Battery technology
- Changes in demand
- Inflation
- 3D Printing
- Safety technology



According to the 2022 The State of Risk Oversight Report from AICPA and NC State, last year 81% of respondents said that their company experienced a significant operational surprise in the past 5 years leading to increased ERM engagement from the Board and Senior Executives.

Source: Beasley, Mark S., and Bruce C. Branson. 13th ed., AICPA, 2022, pp. 9, *2022 The State of Risk Oversight*.

KPMG's approach to risk management includes a coordinated series of activities designed to help identify and proactively respond to these disruptive changes....

Evolving risks

The following describes common evolving risks that are faced by organizations today.

Geopolitical

Uncertainties in the political, environmental, social, and/or macroeconomic environment has driven organizations to prioritize resiliency efforts in order to stay competitive in today's evolving risk landscape

Energy Transition

Global shift from fossil fuels to renewable energy sources with focus on system reliability and resiliency driven by addressing climate change and greenhouse gas emissions as well as an aging and failing nationwide infrastructure

Generative AI

Rapid momentum of technologies that create quality content with minimal human effort has led to concerns over data privacy, ethical standards of the tool, employee misuse, and errors

Consumer Behavior & Loyalty

Changing consumer preferences, attitudes, and expectations towards goods or services as a result of post-pandemic mentality and new generation of customers

Product Development

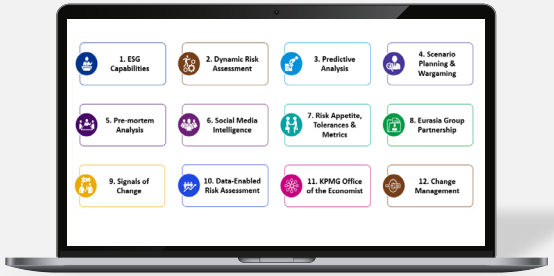
Product development delays and increased material costs due to inflation, supply chain challenges, and economic uncertainty

Business Resiliency

Altering nature of threats to businesses, and the need for businesses to be prepared to respond to a wide range of disruptions

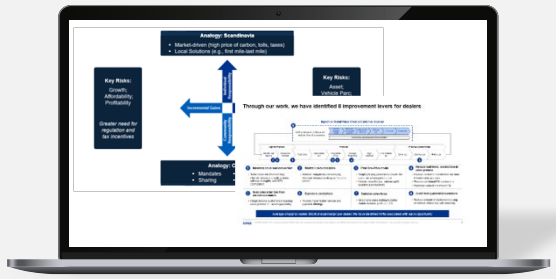
Enterprise Risk Management program trends

ERM is also changing to address emerging challenges and opportunities. Key capabilities to respond to trends focus on:



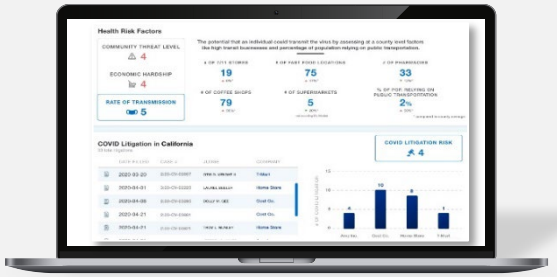
Strategic Capabilities

Organizations are focusing on strategic risk management capabilities and linking risk to the strategic objectives



Scenario Planning and Wargaming

Growing utilization of scenario planning and wargaming techniques to simulate and strategize potential risk scenarios, establish proactive decision-making, and mitigate the impact of unforeseen events



Risk Metrics and Dashboarding

Risk metrics and aggregated dashboarding to drive data-driven insights and provide ongoing monitoring of top risks


ERM Program Comparison

In an effort to determine the optimal desired state of the ERM program, Company's industry, size, and placement of ERM activities within the organization has been compared to that of four other companies. The following table depicts the comparison:

Company	Industry	Footprint	ERM Ownership	# of FTEs	Revenue (in Millions)	Additional Commentary
Company	Technology	Global	TBD	TBD	$1,800	• See current state summary
Company A	Fintech	Global	ERM	4	$1,500	• Full risk assessment program • Advanced ongoing monitoring
Company B	Fintech	US-Focused	CRO	2	$1,000	• Advanced ongoing monitoring
Company C	Data Analytics	US	CRO	3+	$5,000	• Siloed program with limited ongoing monitoring; efforts currently underway to centralize and standardize
Company D	Technology	Global	ERM	5+	$1,200	• Limited ongoing monitoring; little to no understanding of potential risk impact

Value-Driven Risk Management

A shift from risk management being an annual exercise or an extension of internal audit or compliance to being a partner to the business by helping to identify, evaluate, and proactively respond to risks

Incorporation of ESG

Given the increase scrutiny around ESG reporting, ESG risk management processes are aligned to enterprise risk management guidance and process

Risk Governance

Evolving board structures accelerated by anticipated SEC rules have pushed organizations to establish dedicated risk functions and management committees for more effective governance and risk reporting

KPMG

Risk assessment and the DRA approach

How we do it

Risk assessment purpose & objectives

Purpose

- To consider the impact potential events may have on strategic objectives
- To identify, assess, and quantify known and emerging risks
- To gain valuable input from you to better understand a Company's complex risk landscape as well as understand any changes that have occurred
- To align the enterprise-wide risk management approach

Objectives

- Develop an understanding of the risks and opportunities that could impact or accelerate our ability to achieve our strategic objectives
- Capture relevant risks not currently encapsulated in the Company's risk register
- Compile an updated risk register based on feedback received from the interviews and survey results
- Reassess the severity, likelihood, velocity and mitigation effectiveness of each of Company's key risks
- Perform an analysis on the survey results and develop a risk report of the findings

Benefits

Short-term Benefits:

- Prioritizes the most critical risks
- Enables a qualitative and quantitative approach to risk identification

Medium-term Benefits:

- Improves understanding of the organization's risks across all levels

Long-term Benefits:

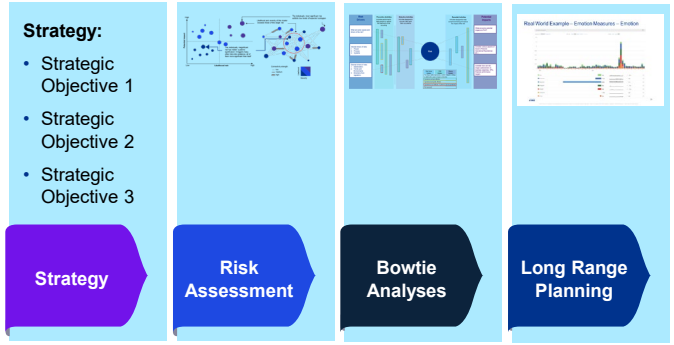
- Enhances management-driven processes
- Elevates risk management capabilities & maturity

Applicability of risk assessment

Strategy | **Enterprise Risk Management** | **Internal Audit**

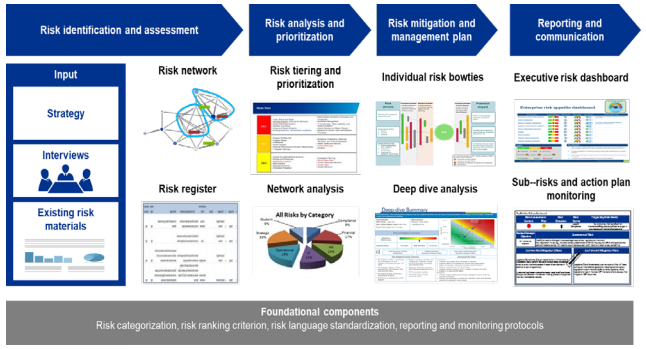
Strategic Alignment

Strategy serves as an input to Risk Assessment. Risk Assessment, in turn, feeds into the strategy.



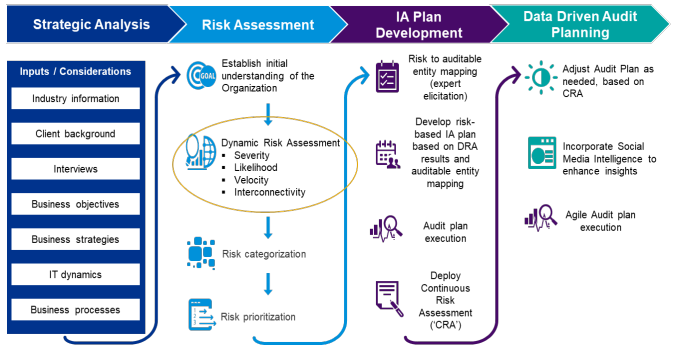
Critical Risks to the Enterprise

Risk Assessments helps risk management functions focus on the most critical risks to the organization.

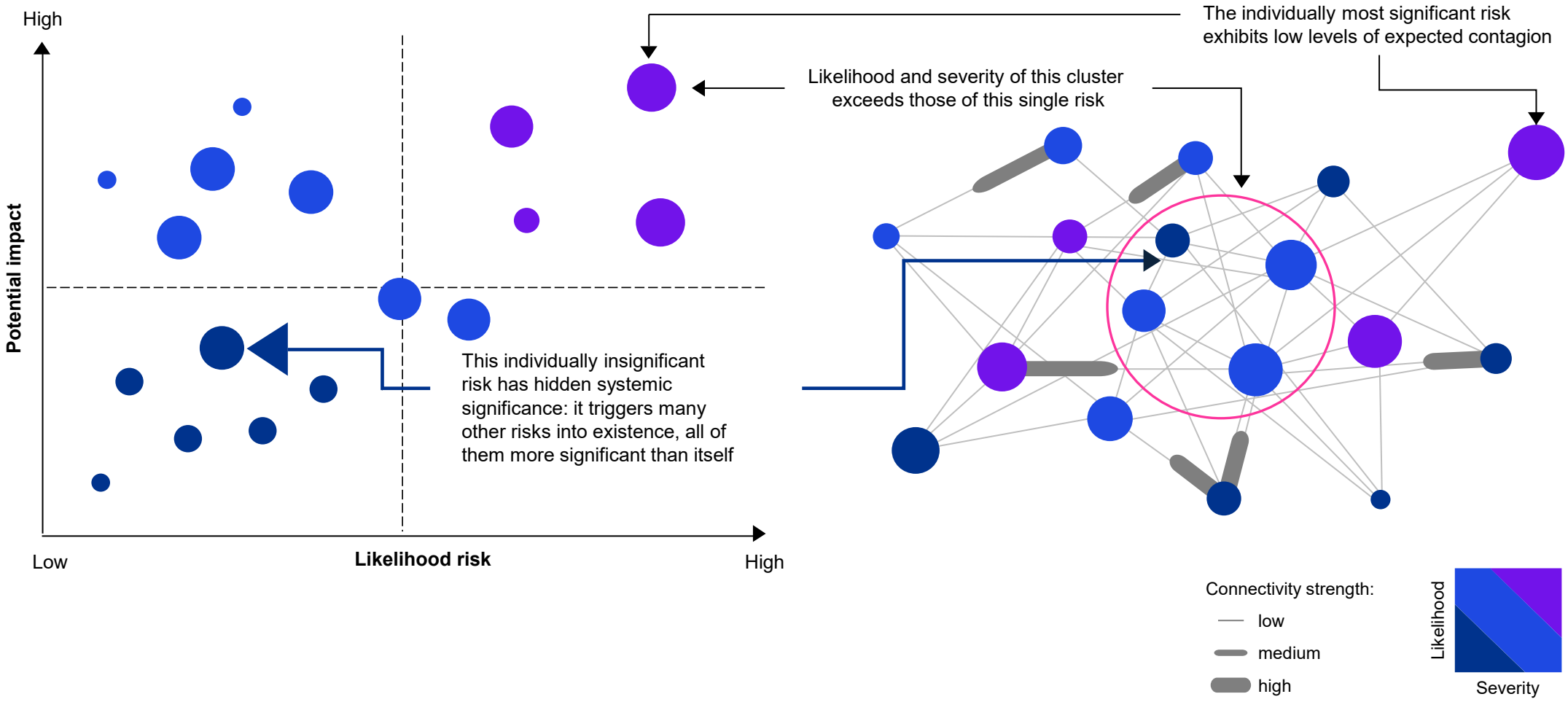


Internal Audit Plan

Risk Assessment fits into an Internal Audit methodology by assisting in the identification, evaluation, and prioritization of critical risks.



DRA – Seeing the difference



The four stages of risk assessment

Planning & Interviews

- Interview senior leaders from across organization to identify risk themes
- Introduce emerging trends and structural breaks to agitate thinking
- Review existing strategy and governance documents
- 6-10 interviews (30-45 minutes)

Workshop #1

- Explore competitive landscape
- Present risk themes which emerged from interviews
- Collectively select top ~15 risks
- 1 workshop with 16+ participants (~1 hour)

Survey and Analysis

- Distribute survey to solicit SMP views on:
  - Severity
  - Likelihood
  - Velocity
  - *Interconnectivity (if DRA)*
- Analyze collective results and create detailed report
- Expected commitment for senior leaders to complete the assessment is ~30 minutes

Workshop #2

- Collectively review and evaluate the results
- Assign risk ownership
- Consider action plans to mitigate identified risks (focusing on root causes)
- 1 workshop with 16+ participants (1 hour)

Risk assessment planning and interviews

Planning & Interviews

- Prior to conducting interviews, frame the scope of risks for the Risk Assessment, leveraging risk content previously created
- Introduce disrupters and signals of change to agitate thinking
- Conduct preparatory interviews with senior leaders ('expert') participants to hone in on key areas of risk to focus on during the 1st workshop (6-10 30-45 minute interviews)
- Develop the initial risk themes listing

Expert Elicitation

- Some of the most valuable insights into future developments and risks can be found through Expert Elicitation.
- Originally developed by the US military to respond to unknown, unprecedented developments behind the iron curtain, it has since developed into an established science.

Why use this approach?

- There is emerging evidence that quantitative risk models present severe limitations in reliably modelling future risks.
- In light of these limitations, it is advisable to use Expert Elicitation to more accurately predict what may happen in the future.
- When performed, the insights gained have proven to be superior to traditional risk modelling methodologies.

Risk assessment planning and interviews - Interviews

No.	Title
1	President, CEO
2	Chief Operating Officer
3	General Counsel
4	Chief Financial Officer
5	Chief Strategy Officer
6	Chief Compliance Officer
7	Chief Human Resources Officer
8	Chief Technology Officer
10	Chief Information Security Officer
12	Global R&D and Marketing Leader
13	Audit Committee Member

Enterprise Risk Assessment Interview Questions

- What must the Company absolutely get right?
- What opportunities are we not taking advantage of that are limiting our success?
- What emerging trends or signals concern you (e.g., disruptive technology advancement, changing business models, etc.)?
- What past trends/cycles do you see as potentially recurring?
- Which known risks are being underestimated?
- What are the most significant risks that might impact the Company?
- Any further comments or observations?

Risk assessment workshop

Workshop 1

- Facilitate workshop 1 with participants (16+ participants for 1 hour)
- Key agenda items:
  - Review workshop objectives
  - Present initial risk themes based on interviews
  - Discuss emerging trends and structural breaks to agitate thinking
  - Brainstorm key risks (~15) and agree on definitions
- Tailor severity risk rating scale criteria to focus on qualitative measures with a translation to quantitative for purpose of aggregation within DRA

Workshop 1 expands on the interviews by considering and identifying potential future risks. Applying the protocol of Expert Elicitation, we:

- Avoid groupthink and “flatten the hierarchy”
- Share “war stories” from other industries and previous employment (rare events)
- Apply imagination to avoid finding only what participants are looking for (confirmation bias)

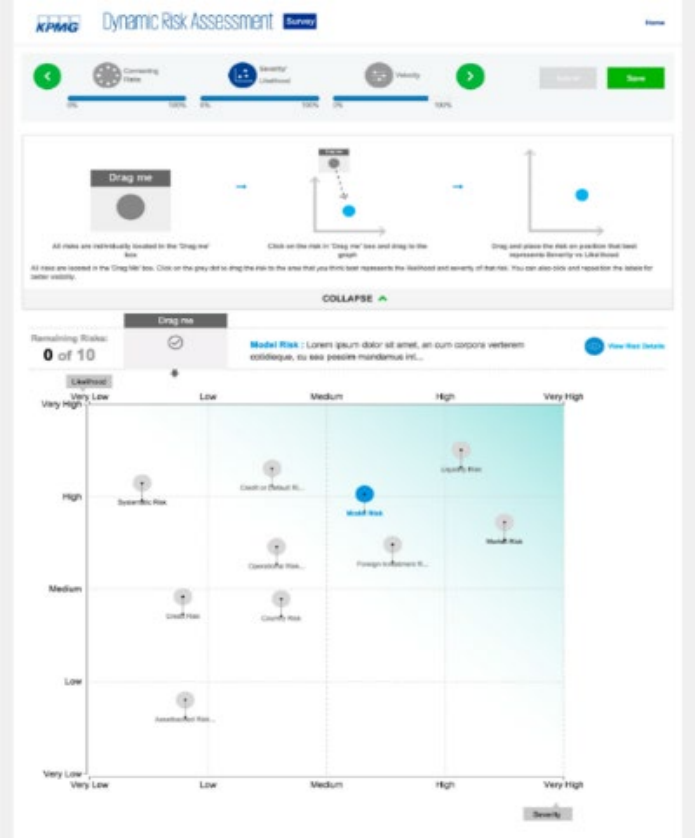
Research shows groups outperform individuals at risk identification and estimation when:

- Diverse views are aired (“consensus not always good/disagreement not always bad”)
- Knowledge feedback occurs through “respectful and helpful clarification”
- Individual response is anonymized but level-set in the group by discussion

DRA collection tool

Question

Rate the severity and likelihood of each risk

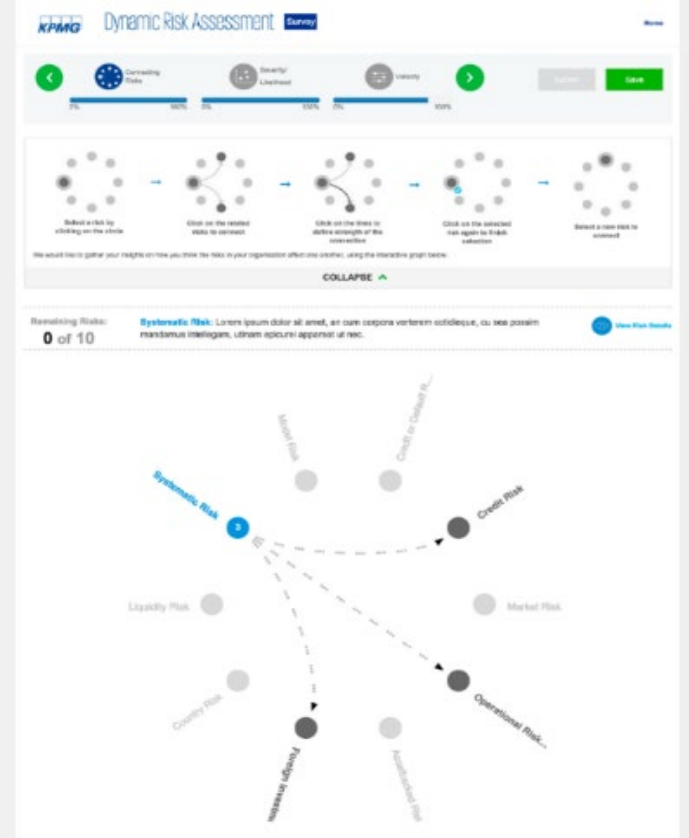


Question

Assess the velocity of each risk (i.e., how quickly it would impact your organization)

Question

Identify how the risks can be expected to connect to each other



DRA report

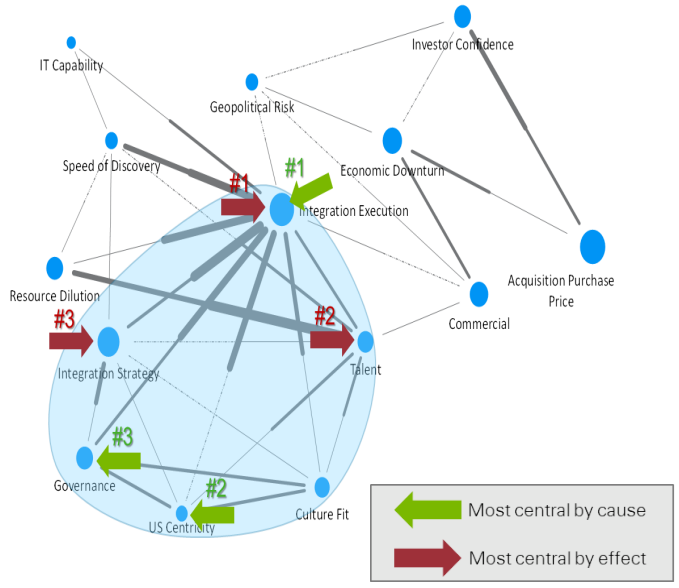
On top of the traditional likelihood-severity plots, the final DRA report consists of:

- risk assessment heat and network maps (multiple dimensions)
- trigger risks
- vulnerable risks
- risk clusters
- in-depth and Client-specific analysis, with interpretation and recommendations.

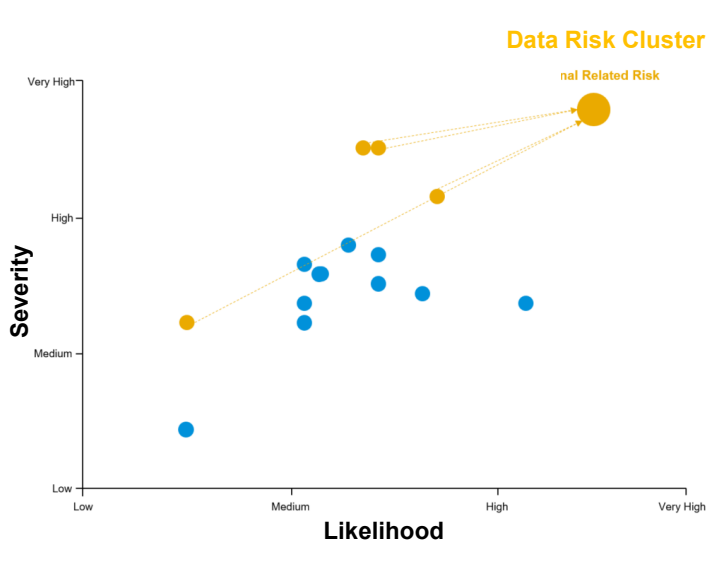
Examples of what kind of graphs will appear in the DRA report can be found on the next few slides. Note that your network will look differently, as no expert elicitation was used for the following networks.

DRA report (cont.)

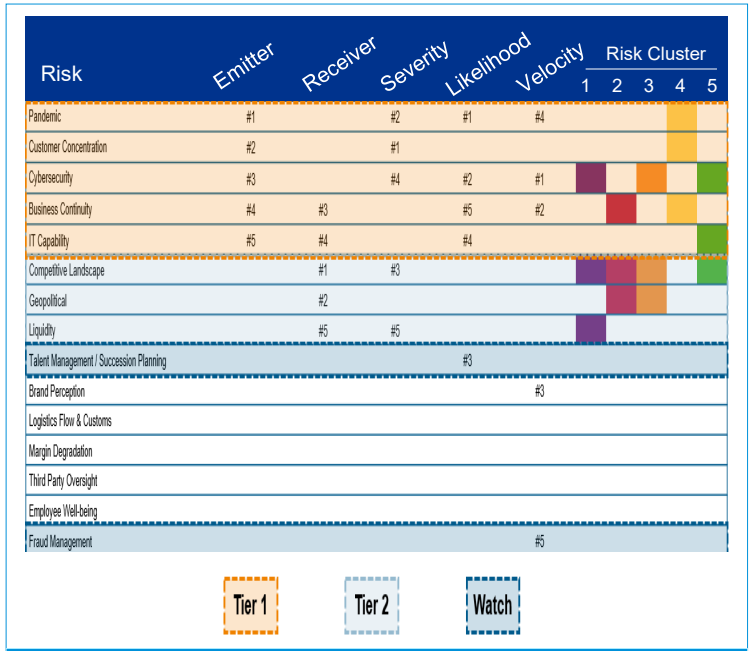
The outputs show how DRA could support identification of the most influential and vulnerable risks to strategic objectives, which can then be aggregated, reviewed based on connectivity, severity, likelihood, and velocity, and prioritized for action.



Risk Emitters & Receivers



Risk Aggregation & Clusters



Executive View of Priority Risks

The four stages of risk assessment

Planning & Interviews

- Interview senior leaders from across organization to identify risk themes
- Introduce emerging trends and structural breaks to agitate thinking
- Review existing strategy and governance documents
- 6-10 interviews (30-45 minutes)

Workshop #1

- Explore competitive landscape
- Present risk themes which emerged from interviews
- Collectively select top ~15 risks
- 1 workshop with 16+ participants (~1 hour)

Survey and Analysis

- Distribute survey to solicit SMP views on:
  - Severity
  - Likelihood
  - Velocity
  - *Interconnectivity (if DRA)*
- Analyze collective results and create detailed report
- Expected commitment for senior leaders to complete the assessment is ~30 minutes

Workshop #2

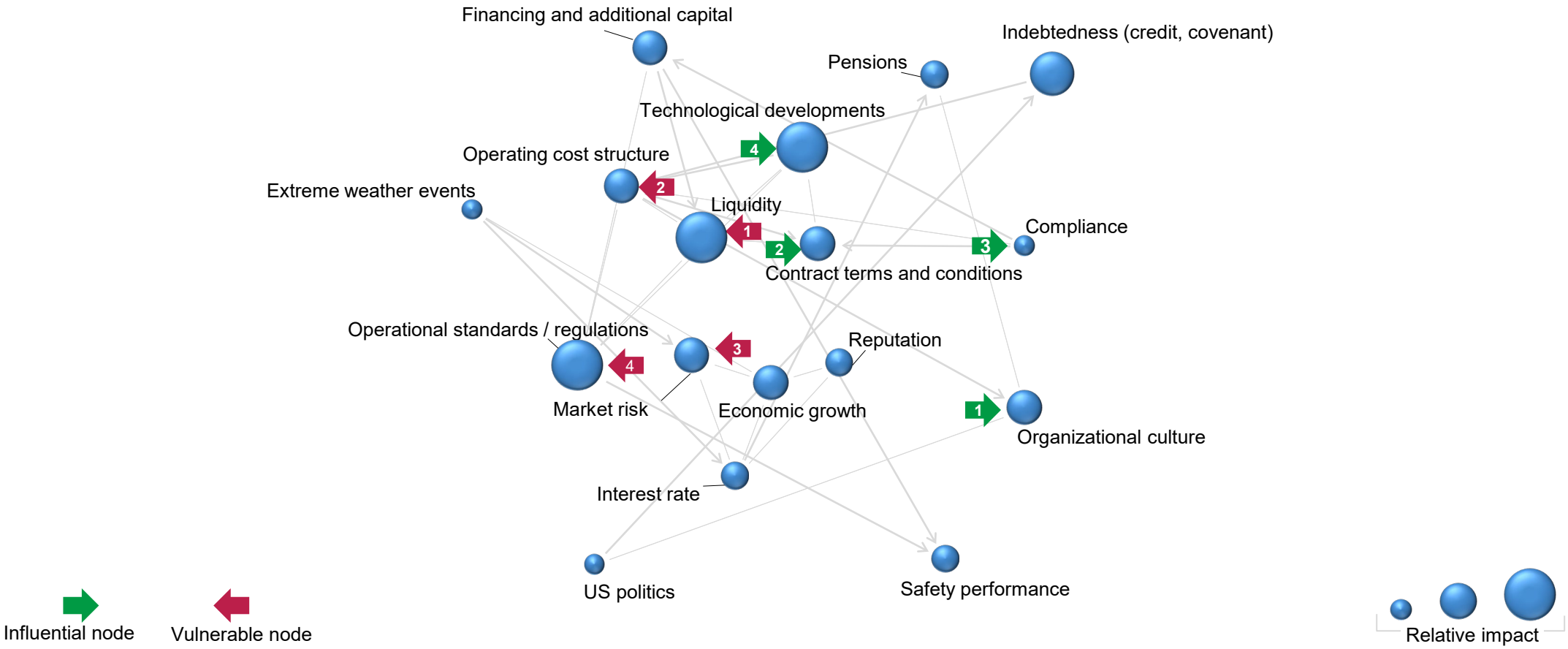
- Collectively review and evaluate the results
- Assign risk ownership
- Consider action plans to mitigate identified risks (focusing on root causes)
- 1 workshop with 16+ participants (1 hour)

KPMG

DRA output

How it leads to better insights

Example output: Influential and vulnerable risks



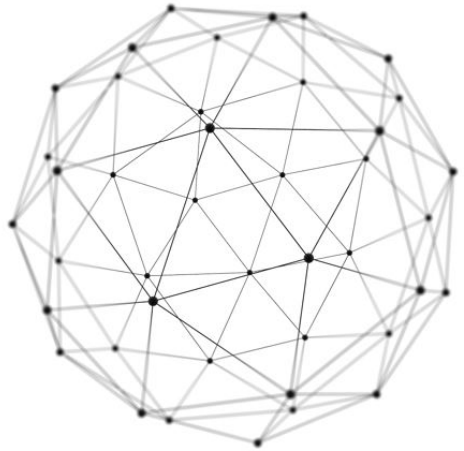
Stylized impression of network depiction. This network is completely hypothetical. No Expert Elicitation was used for its creation. Positions and node names in the network have been selected randomly, and so no reasonable conclusions can be drawn from this example.

Organizational benefits

When targeted on the enterprise, a transformation, or a business unit, DRA supports quantified capture of leadership's views to highlight risk and opportunity. DRA:

- Captures relevant information
- Creates understanding for **alignment across departments**
- Allows leadership to **capitalize on interconnectedness** between risks
- Helps management to **focus on the crucial** without overlooking important issues

DRA leads to a more accurate, forward-looking assessment, enabling highly effective strategy setting and risk management policies that enjoy wide support.



Outputs can be operationalized to support a range of enhanced risk-based analyses and practices

Scenario Planning

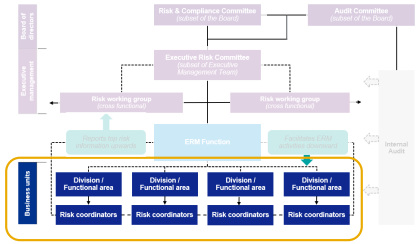
Use risk clusters to better inform scenario planning

- Identify and evaluate causal factors that determine alternative end-states
- Combine DRA outputs to better define consistent scenarios
- Analyze business implications of each scenario
- Develop portfolio of potential actions for each scenario

Risk Governance

Holistic management and accountability of connected risks

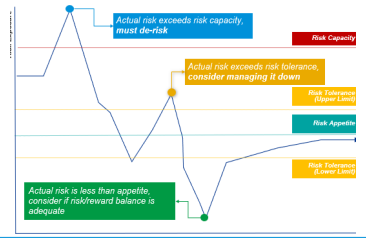
- Identify risk stakeholders across the risk clusters
- Provide awareness training on risk clusters and connectivity
- Make teams accountable for risk clusters
- Incorporate cluster information into risk-based decision-making processes and controls



Connected Risk Monitoring

Identify and link early warning indicators

- Identify the most vulnerable and influential risks corresponding risk metrics
- Link metrics to identify potential triggers with broad implications earlier
- Develop reporting dashboards that show coordinated risk indicators across risk clusters
- Take into account velocity in choosing indicators and prioritizing responses



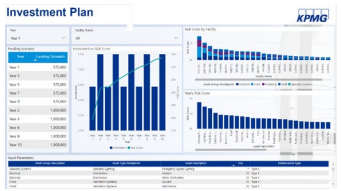
Capital Planning

Apply risk-based capital planning informed by connected risks

- Use DRA network to simulate allocation of total spend across the network
- Compare with financially constrained capital plan

Going one step further…

- Use a risk-based capital prioritization tool in lieu of the current, static capital plan
- Run variable funding scenarios to test investment strategies vs. risk tolerance

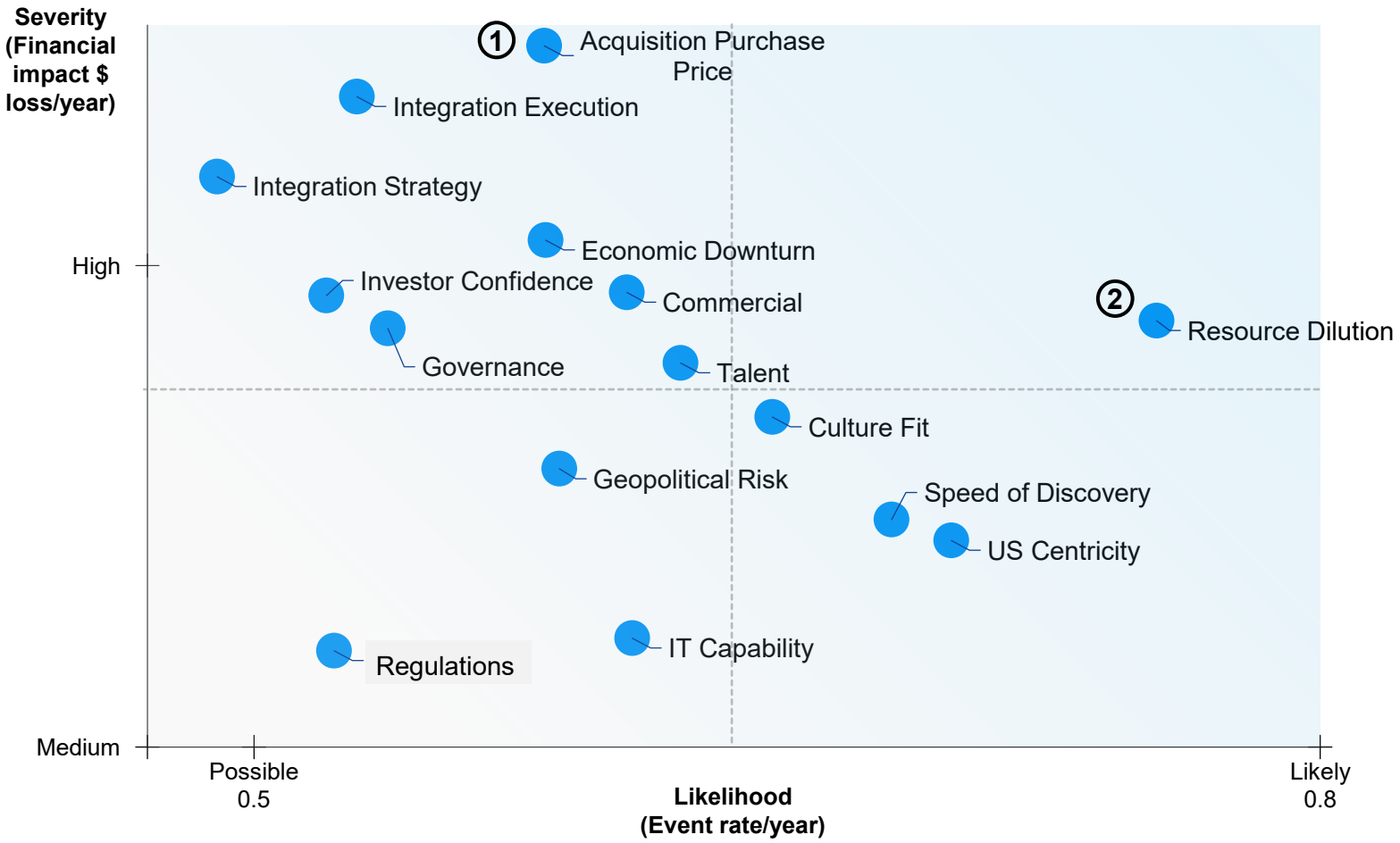


Previous DRA impact

Differentiated results

Case study

Severity and Likelihood



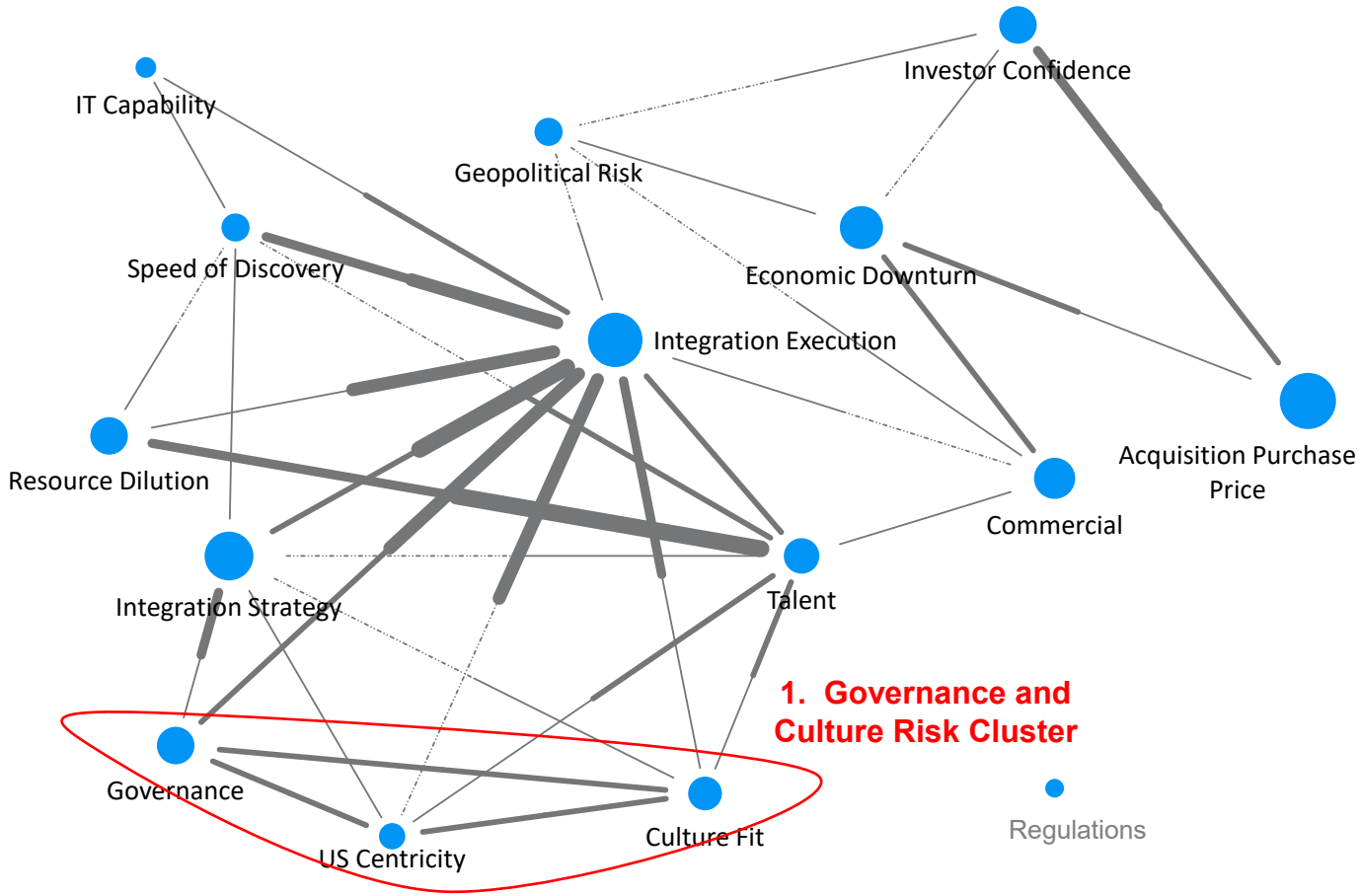
- This client performed a strategic risk assessment for major acquisition in Europe.
- Pricing of the deal is always top of mind.
- This was confirmed by the 2-dimensional plot, that ranked Acquisition Purchase Price as highest in severity and Resource Dilution (moving senior leaders abroad) as most likely.

① *Acquisition Purchase Price* is perceived to be the most severe risk in the network, with high consensus on the estimate.

② *Resource Dilution* is perceived to be the most likely risk in the network, also with relatively high consensus on the estimate.

Case study

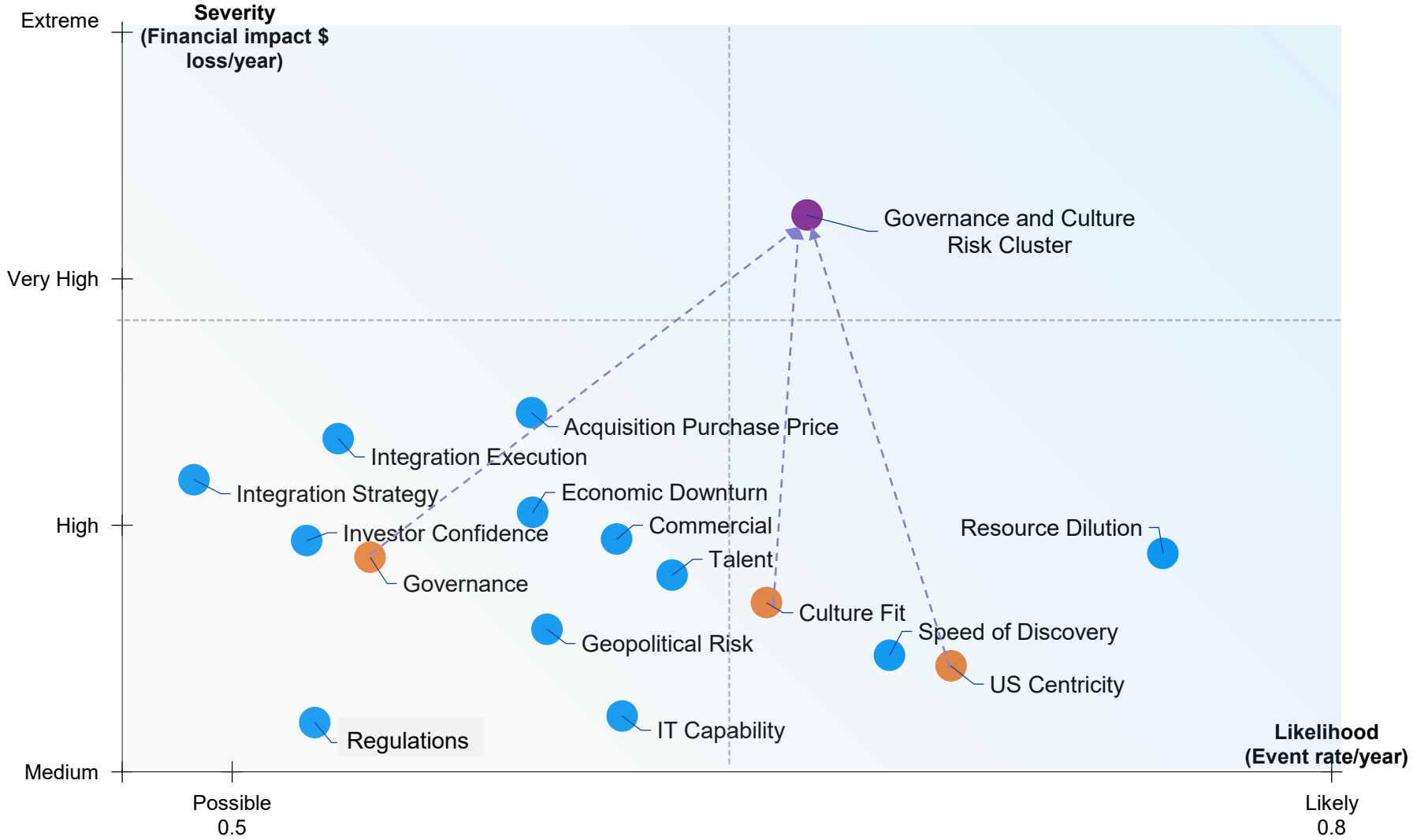
Risk interconnectedness



- The network view revealed new insights.
- **Purchase price was not connected to other risks.** It could be managed by itself.
- Several risks clustered together into a Governance and Culture Risk cluster that could broadly impact success. The trans-Atlantic **synergies hinged on governance and culture.**

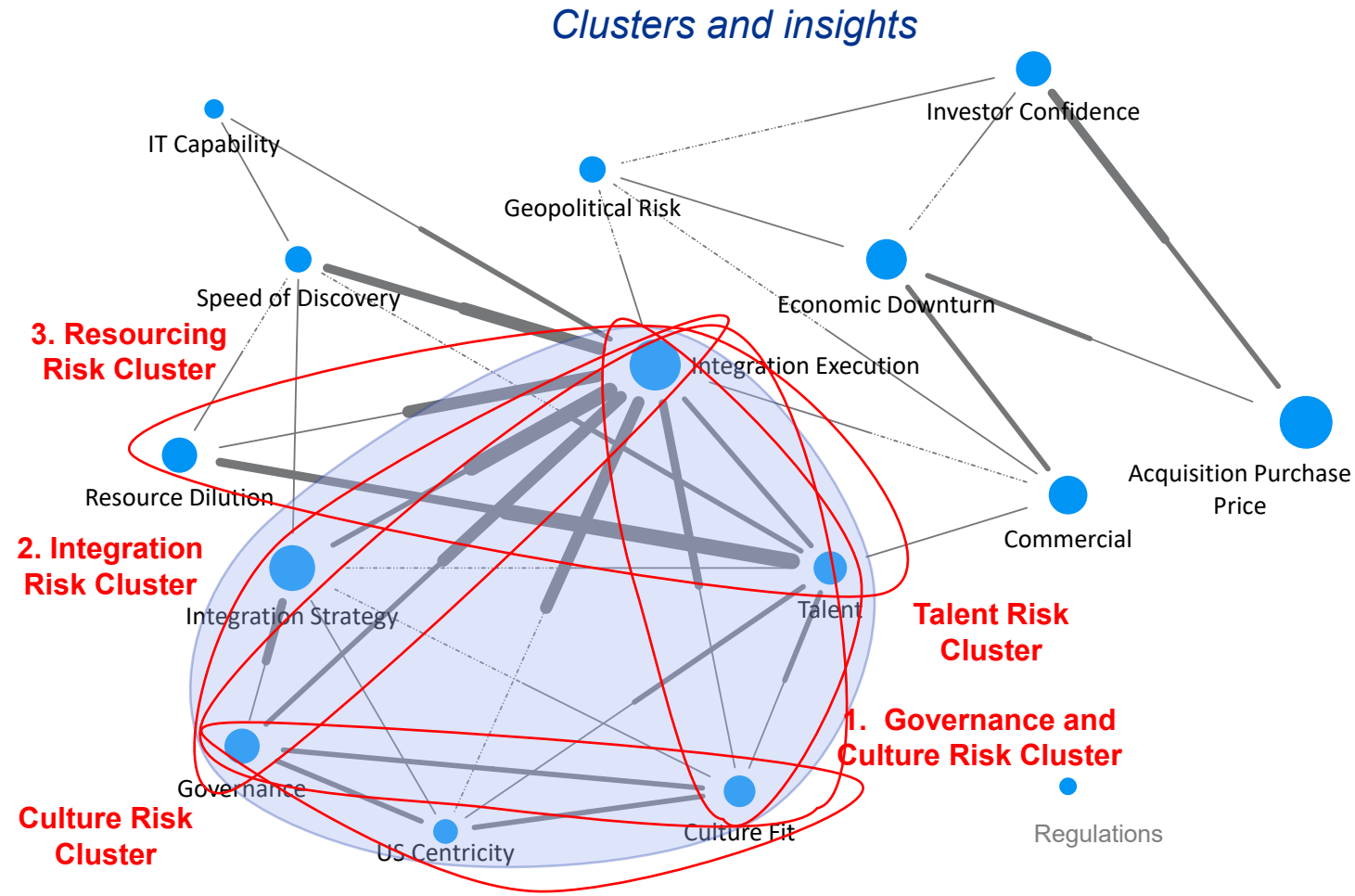
Case study

Combined cluster impact

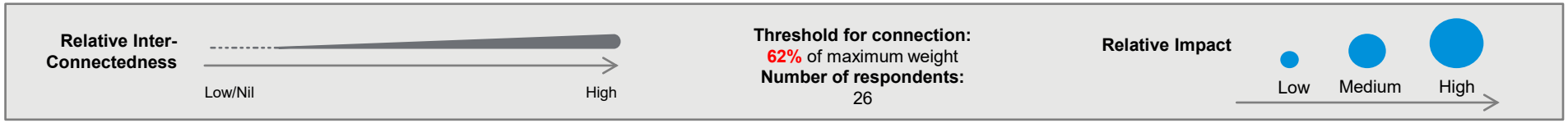


In fact, total impacts of this **cluster was more severe than** any other risk, including **Acquisition Purchase Price**.

Case study

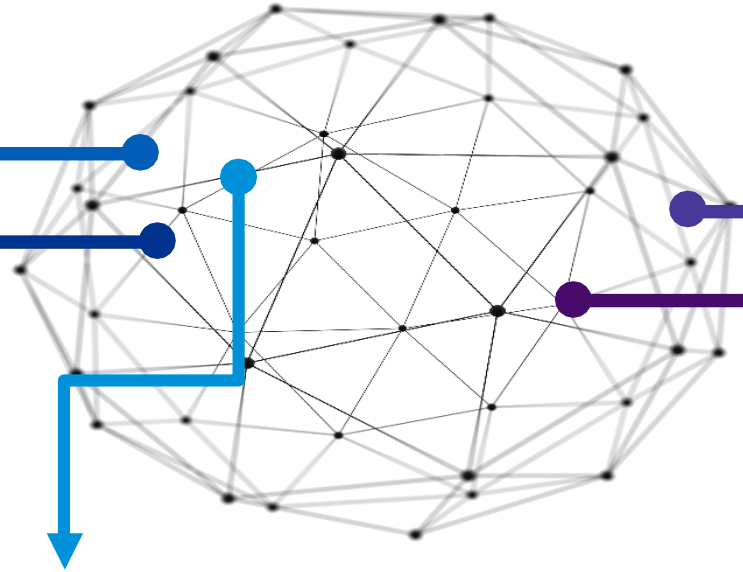


- There were also several strong connections with integration risks.
- This led to the key strategic insight that for this deal to be successful in the long run, the company needed to let go of simply "chopping off the head" and inserting US management structures.
- It would have to transform into a "two-headed" entity, leaving the culture and governance of the European entity intact.



Other DRA use cases

Below are some anonymized examples of previous client cases, to illustrate how DRA leads to added and actionable insights on strategic, cultural, management, and operational levels.



1

Build vs. buy decision in an industrial manufacturing company

- **DRA identified**: Estimated market actions taken by competitors groups for two scenarios.
- **Insights:** Management identified most appropriate actions based on likely market actions take by competitor groups and market participants that were and were not understood
- **Actions taken**: Decision to buy vs. build and related mitigation steps were solutioned based on results

2

Organizational change in a technology company

- **DRA identified**: Few connections between two parts of the network (i.e., almost two separate networks).
- **Insights**: A disconnect between two key parts of the organization, resulting from a recent reorganization.
- **Actions taken**: Improved integration with the disconnected departments via talks with managers, improving internal communication, and change management policies according to feedback.

3

Rethinking competition for a major airline

- **DRA identified:** An impactful vulnerable risk, i.e., the organization had little influence there.
- **Insights**: Management realized it could not compete in this area.
- **Actions taken**: A strategic shift to partner with a competitor in this area instead of trying to compete.

5

Cultural aspects in a financial company

- **DRA identified:** Tone at the top as a key root cause for reputational and fraud risks, thanks to the anonymous collection tool.
- **Insights**: The risk calculations showed how impactful leadership tone was.
- **Actions taken**: Management discussions led to a new ethics framework, including implementation of 360 degree evaluations.

4

Influential risk for a car manufacturer

- **DRA identified:** Regulation as an insignificant risk by itself, but highly influential in the network.
- **Insights**: Regulation was recognized as crucial instead of a compliance issue, and could be turned into an opportunity.
- **Actions taken**: The influence of the risk was leveraged by using outperformance in this risk area to distinguish the company from its competitors.

Thank you

Joey Gyengo
US Enterprise Risk Management Leader
(404) 520-5327
jgyengo@kpmg.com

Diana Griffin
IAER Risk and Innovation specialist
(843) 814-3322
dianagriffin@kpmg.com

kpmg.com/socialmedia