



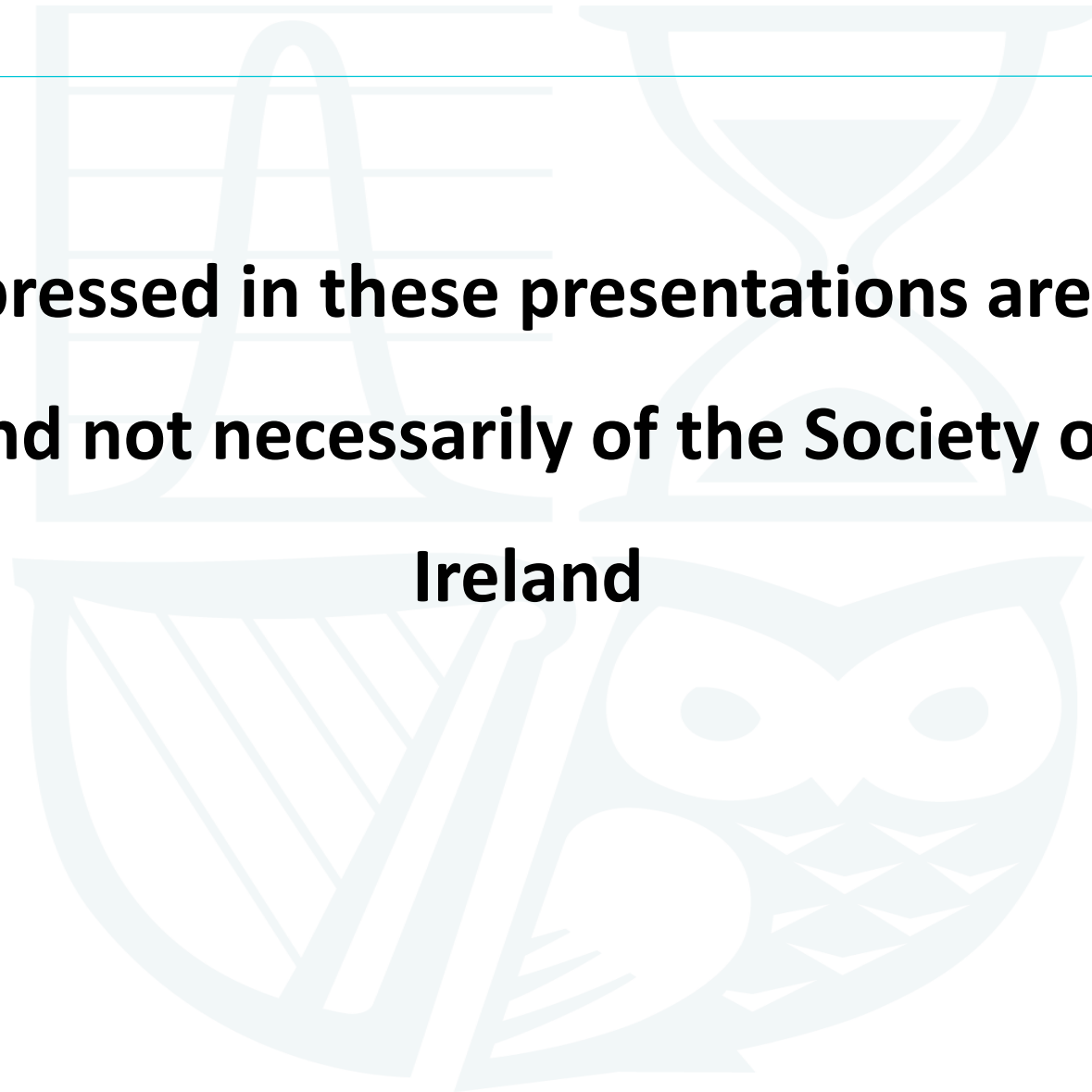
Society of Actuaries in Ireland

**Risk Management Perspectives
Conference 2018**

12th October 2018

Disclaimer

The views expressed in these presentations are those of the presenter(s) and not necessarily of the Society of Actuaries in Ireland





Society of Actuaries in Ireland

Welcome & Introduction

Maurice Whyms



Google Trends: “scandal”

(IRELAND)

● scandal
Search term

+ Compare

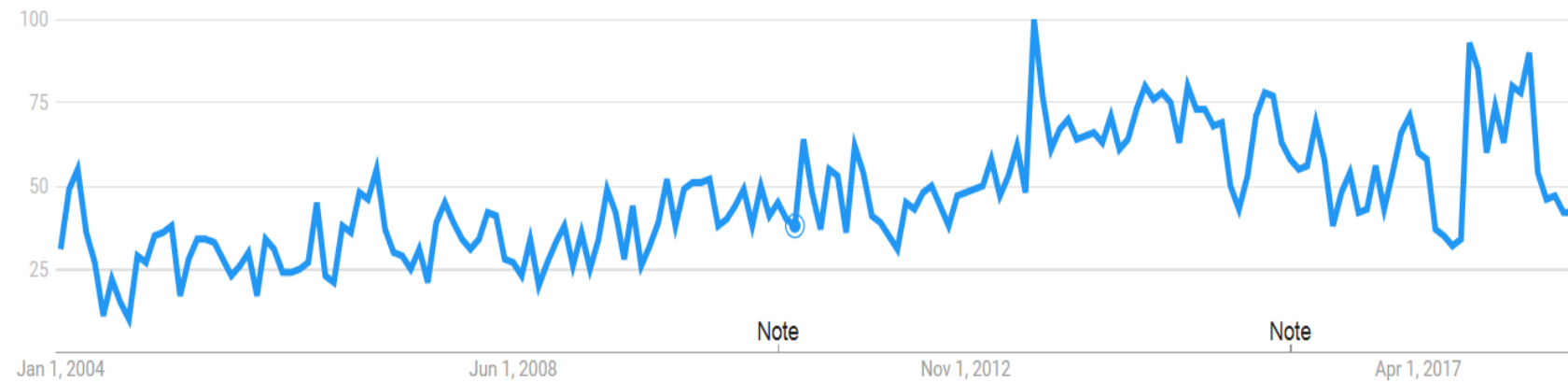
Ireland ▼

2004 - present ▼

All categories ▼

Web Search ▼

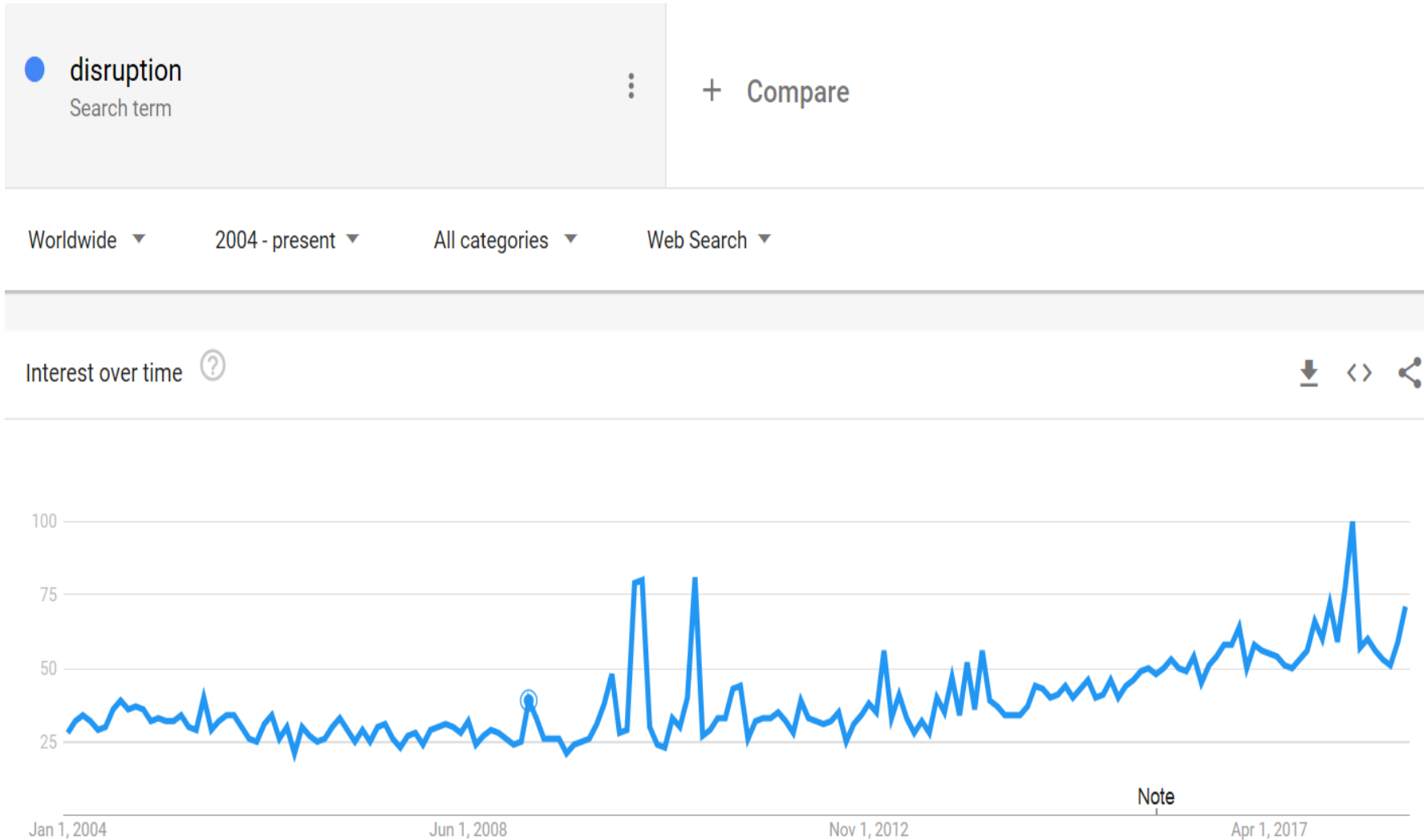
Interest over time ?





Google Trends: “disruption”

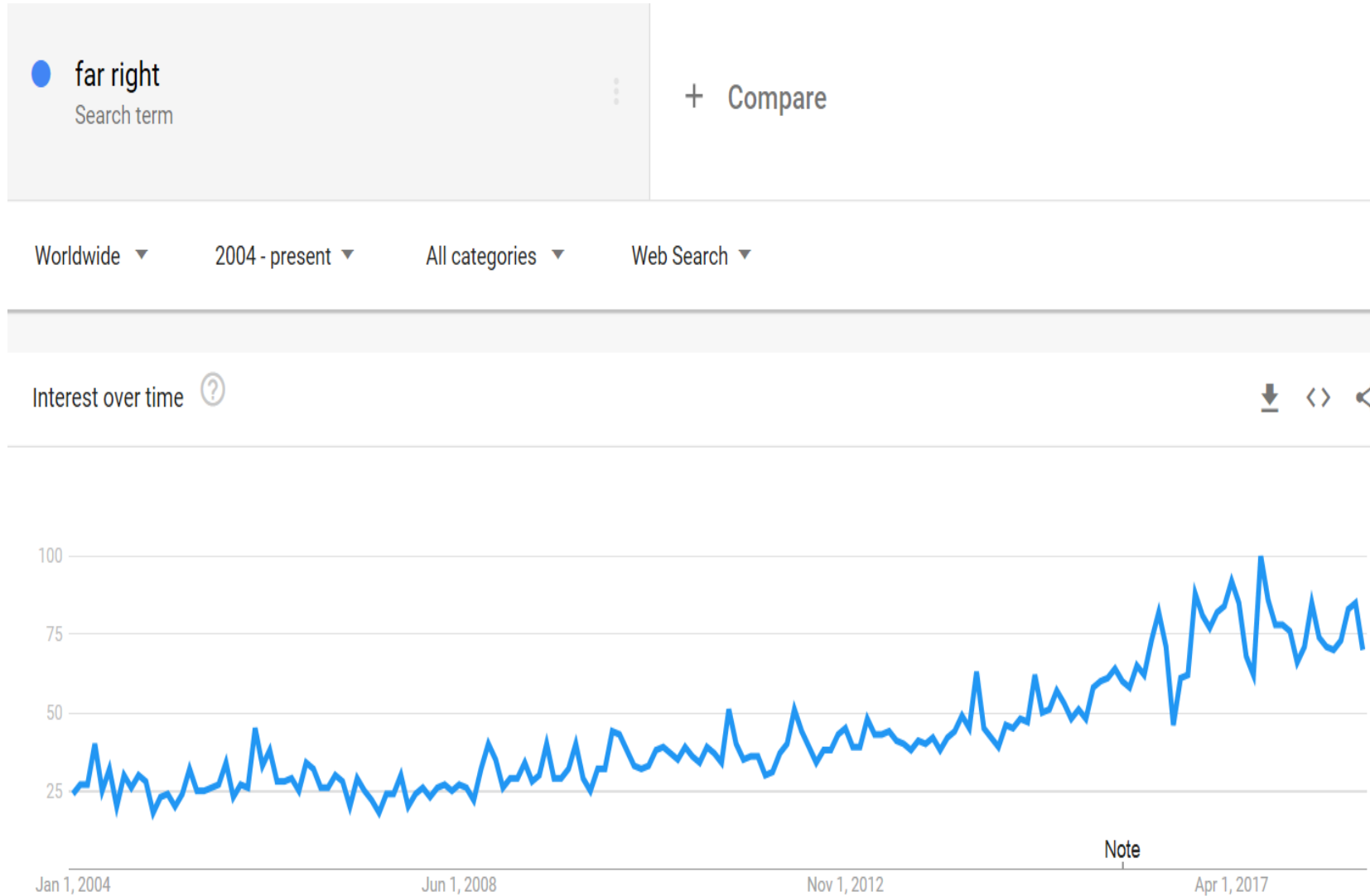
(WORLDWIDE)





Google Trends: “far right”

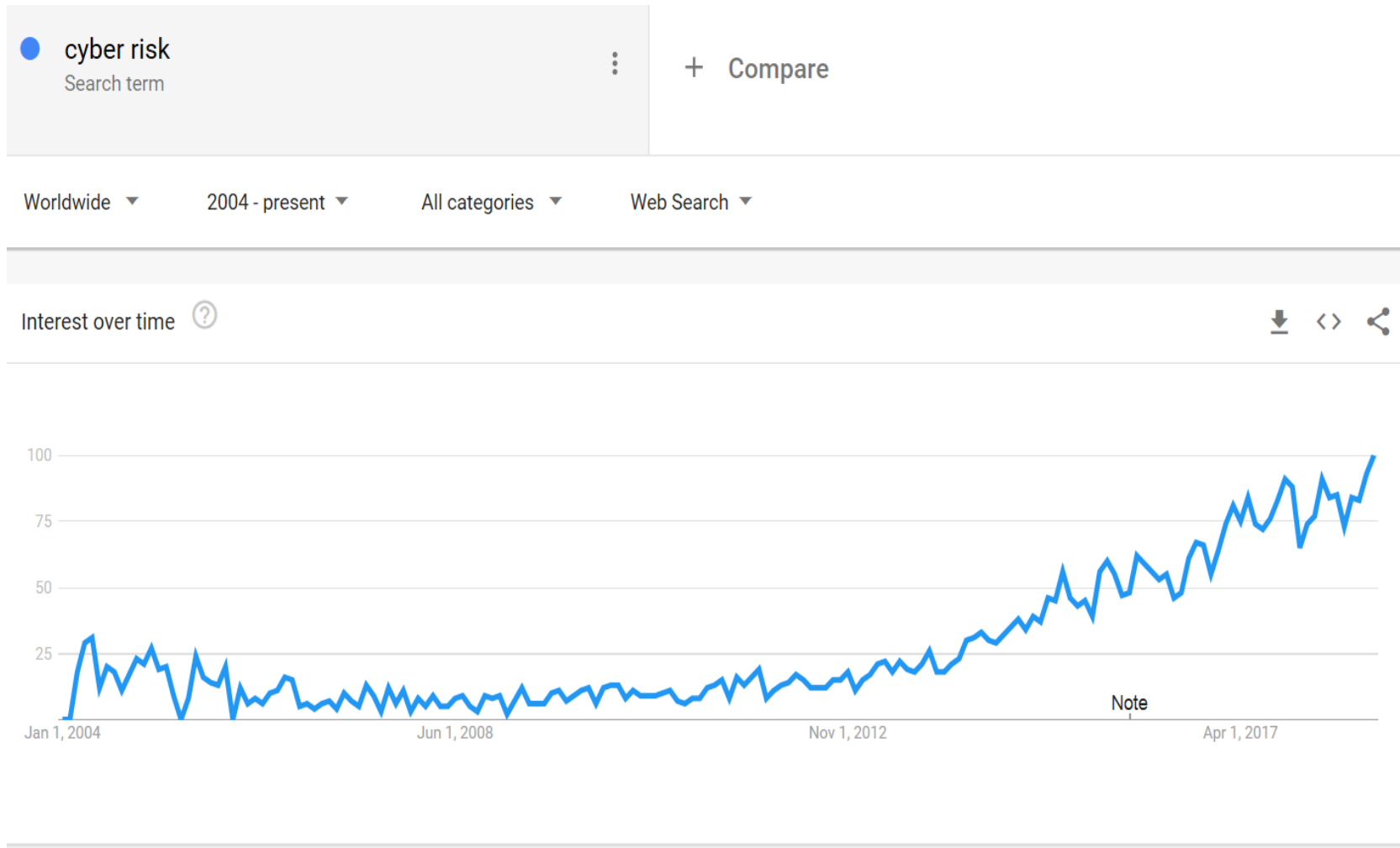
(WORLDWIDE)





Google Trends: “cyber risk”

(WORLDWIDE)





Google Trends: “recipe” (IRELAND)

● recipe
Search term




+ Compare

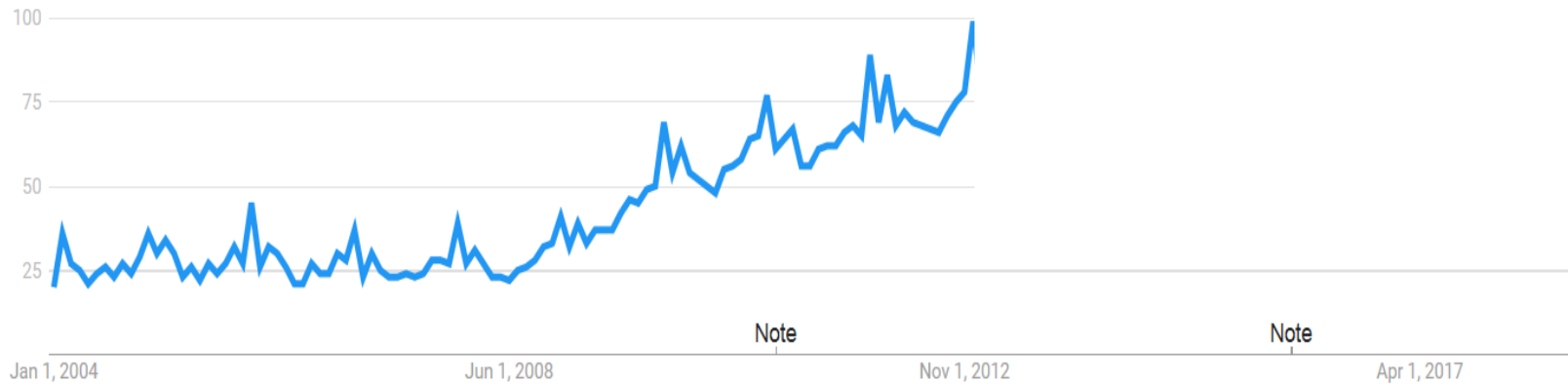
Ireland ▾

2004 - present ▾

All categories ▾

Web Search ▾

Interest over time 





Google Trends: “recipe”

(IRELAND)

● recipe
Search term

+ Compare

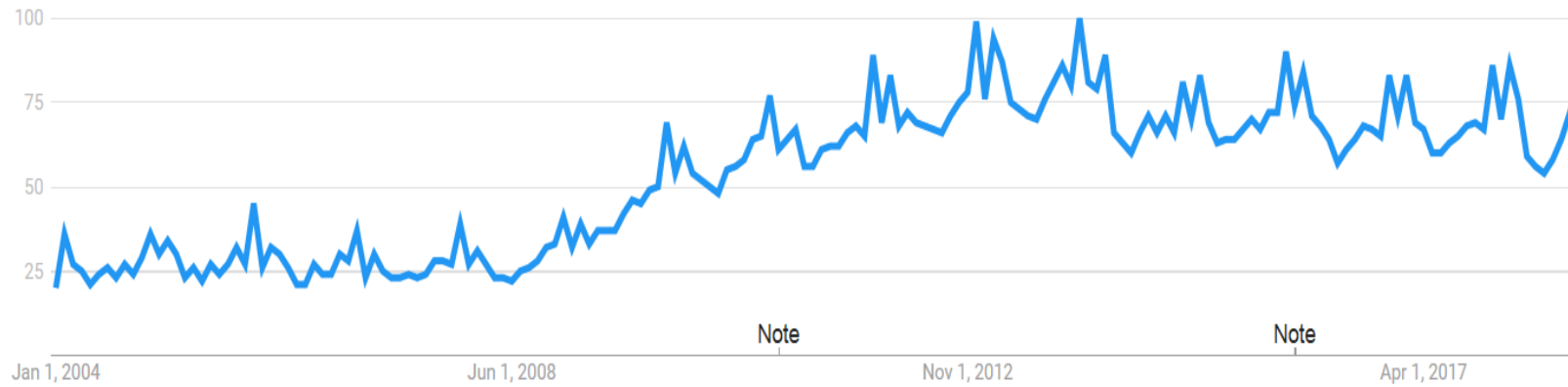
Ireland ▼

2004 - present ▼

All categories ▼

Web Search ▼

Interest over time ?





- Library can be found here: <https://web.actuaries.ie/press/erm-library>
- Currently has over 800 papers on Enterprise Risk Management
- The Library is undergoing a review, with up to 250 papers being added
- New additions cover a variety of topics including:

Interest rate risk

Extreme event
risk

Emerging risks

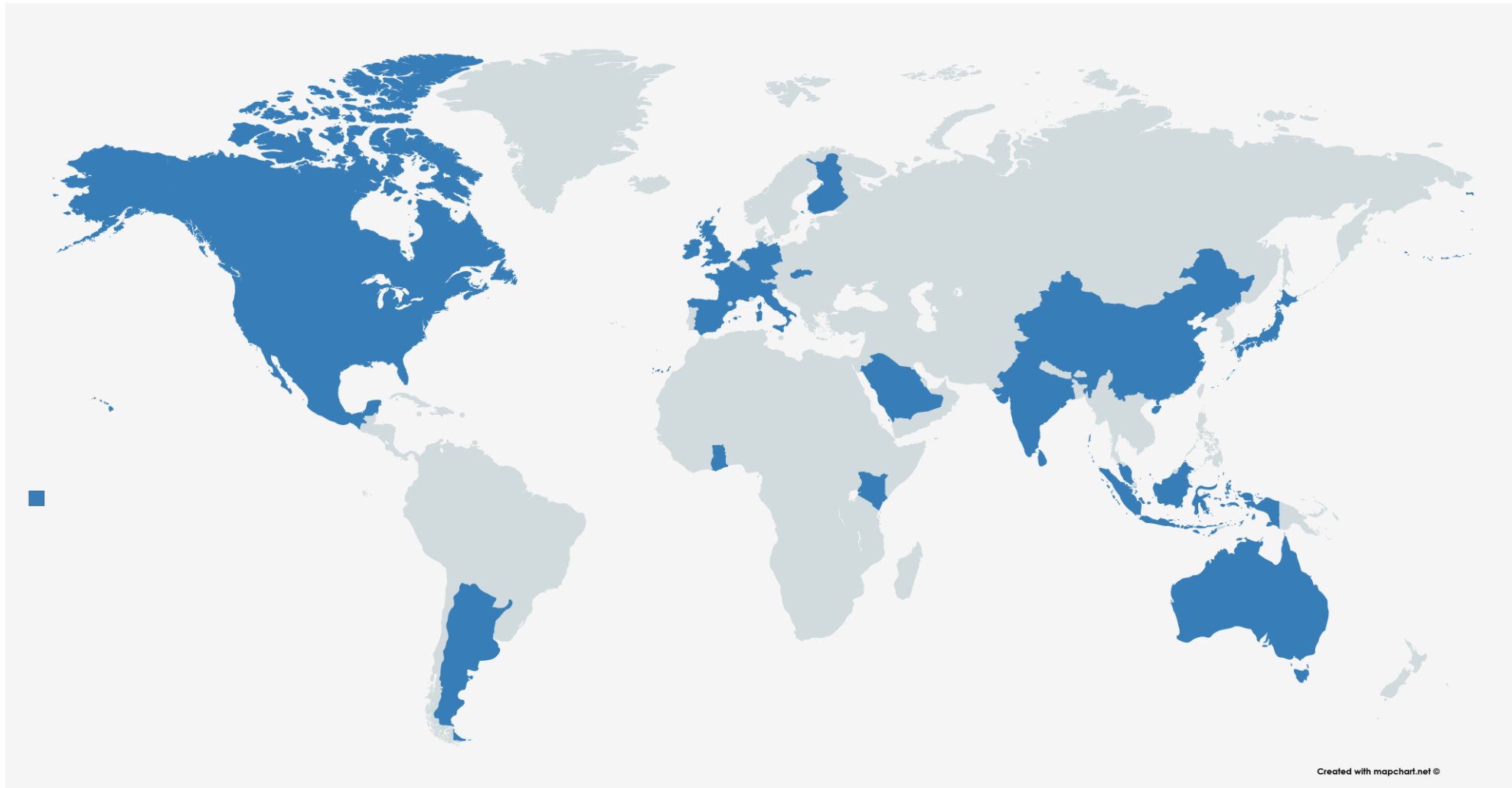
Cyber risk

Risk culture

Conduct risk

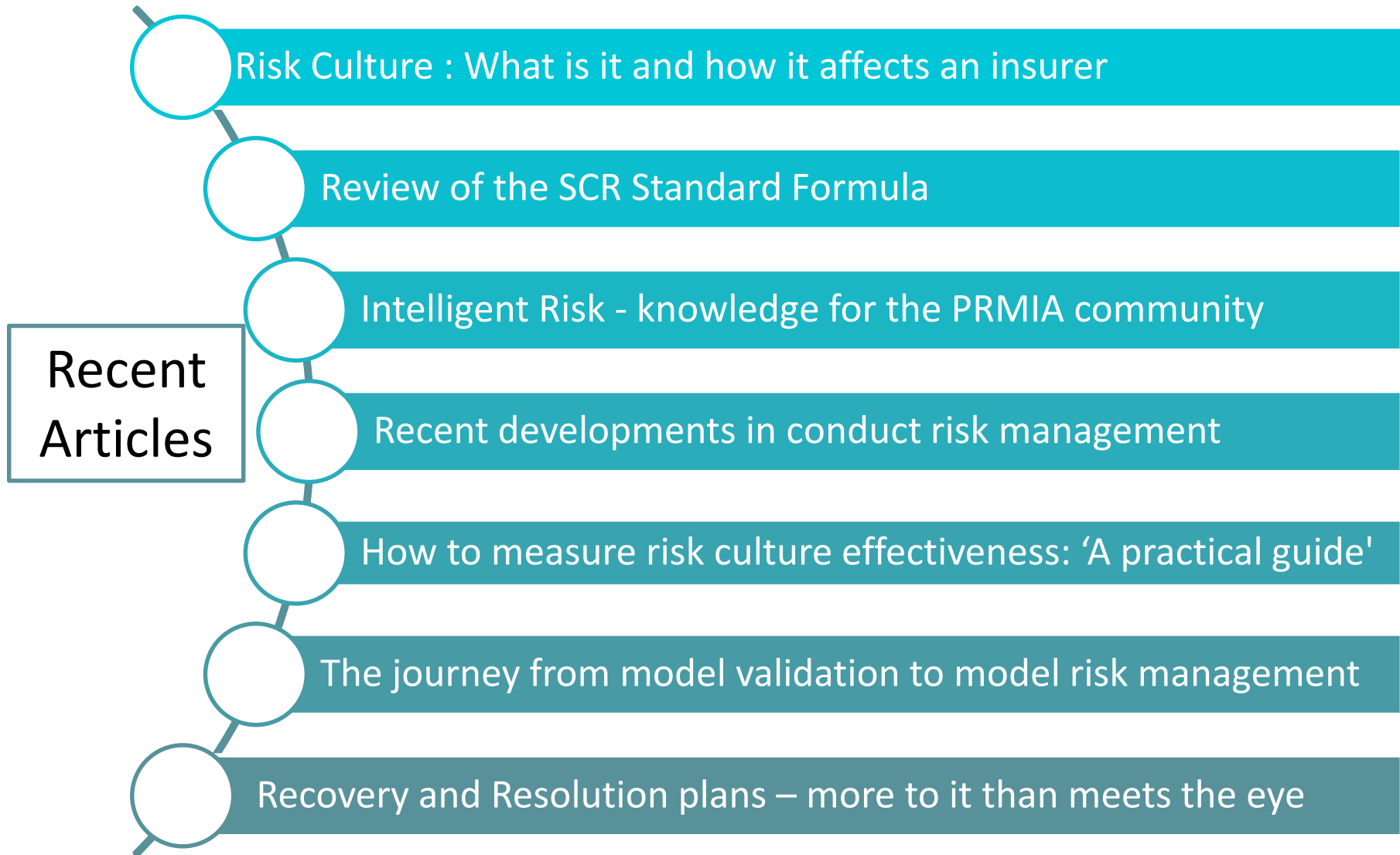


In the past year, the Library has had over 7,000 visitors from all around the world including US, UK, Australia, Mexico, Germany, Switzerland, Italy and Japan.





Find us on LinkedIn!



Agenda

8:00 – 8:30	Registration & coffee	
8:30 – 8:45	Welcome and introduction	Maurice Whyms (President of the Society of Actuaries in Ireland)
8:45 – 9:20	Brexit update	Senator Neale Richmond
9.20 – 9.55	Aligning operational risk and insurance	Thomas Jaeggi (Marsh), Angelos Deftereos (XL)
9.55 – 10.30	Risk functions: keeping pace with data analytics	Jean Rea (KPMG)
10.30 – 10.50	Coffee	
10.50 – 11.30	Reliance Board places on the risk team to prepare a good ORSA	Brenda Dunne (INED)
11.30 – 12.15	Panel discussion – Perspectives on risk culture	Jennifer Minogue (Central Bank of Ireland), Sean Casey (INED), Brian Binchy (EY), James Maher (EY – chair)
12.15 – 13.15	Lunch	

Agenda (continued...)

After Lunch		
13.15 – 13.50	Geopolitical risk and Macroeconomic update	Jim Power (Jim Power Economics Ltd.)
13.50 – 14.25	Cyber Risk Scenarios for Insurance Companies - IFoA Working Party Update	Patrick Meghen (Milliman)
14.25 – 14.40	Coffee	
14.40 – 15.15	2 nd Line of Defence perspective on Regulatory Reporting	Dr Allan Kearns (Central Bank of Ireland)
15.15 – 15.50	Consumer protection risk	Brian Binchy (EY)
15.50 – 16.00	Closing remarks	Maurice Whyms



Society of Actuaries in Ireland

Aligning Operational Risk and Insurance

Angelos Deftereos (AXA XL), Thomas Jaeggi (Marsh)



Introduction

Topics to be covered

1. Aligning operational risk and insurance
2. Incorporating insurance into models
3. Operational risk insurance

Speakers

- Angelos Deftereos - Head of Operational Risk - International Financial Lines, AXA XL
- Thomas Jaeggi - Head of Risk Advisory for Financial Institutions, Marsh UK

Internal Model Industry Forum:
Aligning Operational Risk and Insurance
April 2018

Internal Model Industry Forum

ORIC INTERNATIONAL

Supporting:

pwc Milliman MARSH

IRIS and Society of Actuaries LCP EY

irm



1. Aligning operational risk and insurance

- Operational risk and insurance are closely related but have historically been seen as separate disciplines
 - Operational risk: “risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”¹
 - Insurance: well-established means to transfer operational risks to third parties
- Aligning operational risk and insurance can achieve a range of benefits, e.g.
 - Determining optimal insurance transfer strategy / programme (including bespoke options)
 - Demonstration of use of risk management framework and models
 - Recognising the risk mitigating effects of insurance for capital purposes
- Under Solvency II, insurance can be used to offset the operational risk contribution to the SCR²

1. Basel definition.

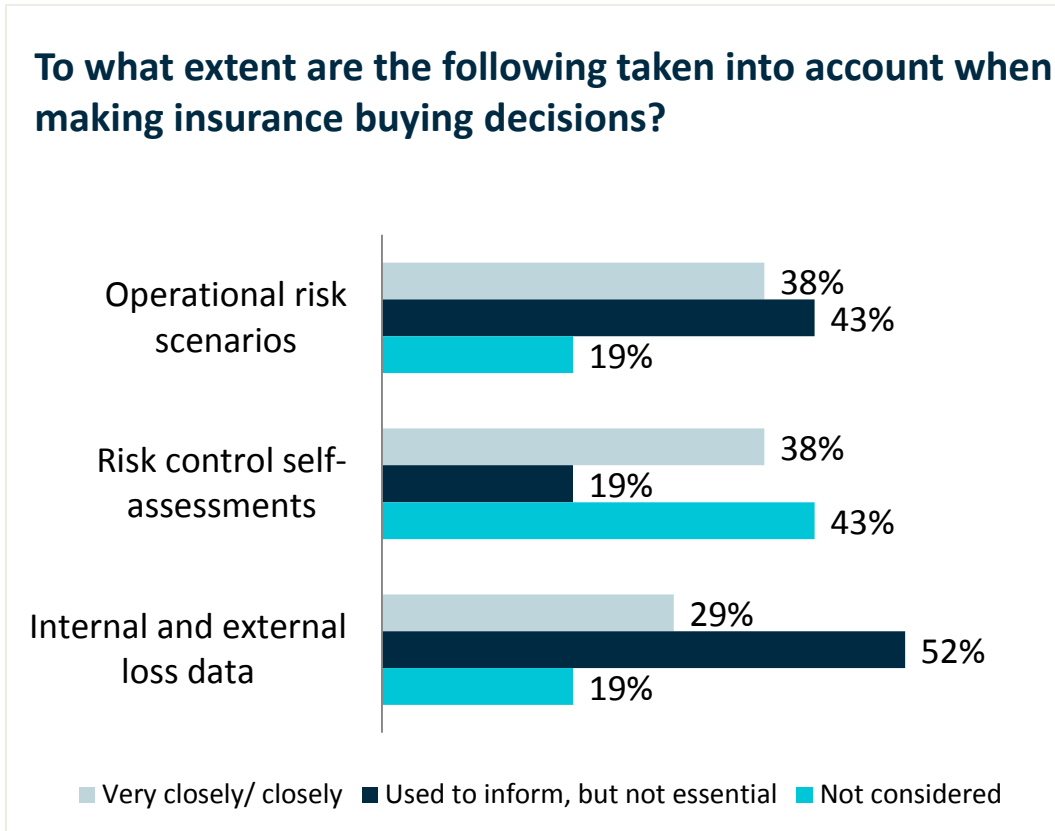
2. Provided that credit risk and other risks arising from the use of such risk mitigation techniques are properly reflected (Article 101(5) of Directive 2009/138/EC (Solvency II)).



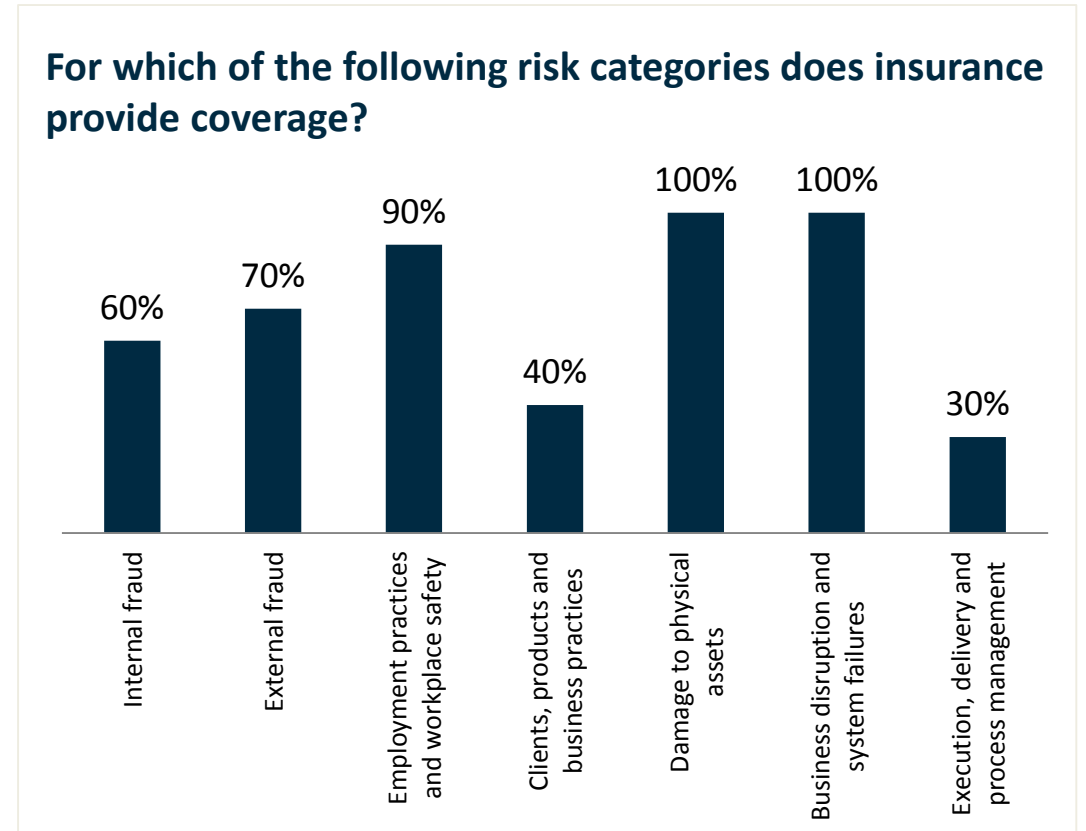
1. Aligning operational risk and insurance

State of the market (1 / 3)¹

Use of op risk processes for insurance purchasing



Risks covered by insurance programmes



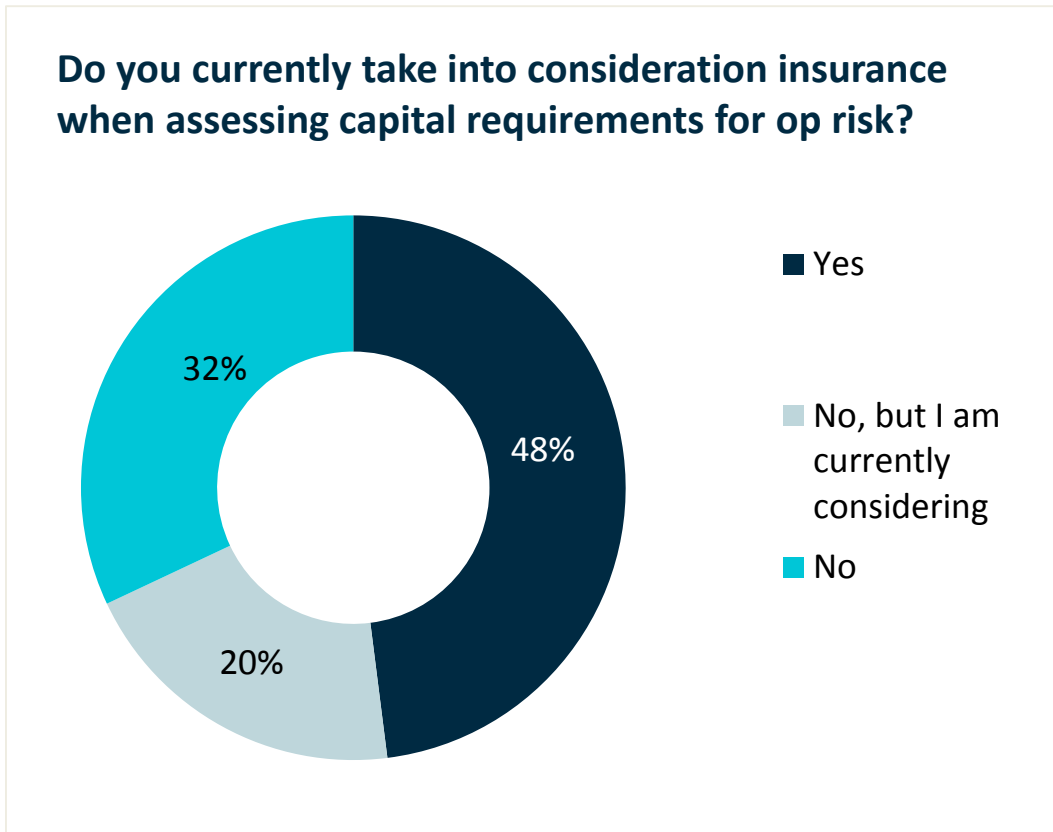
1. Based on survey of 25 insurers conducted during Q4 2017.



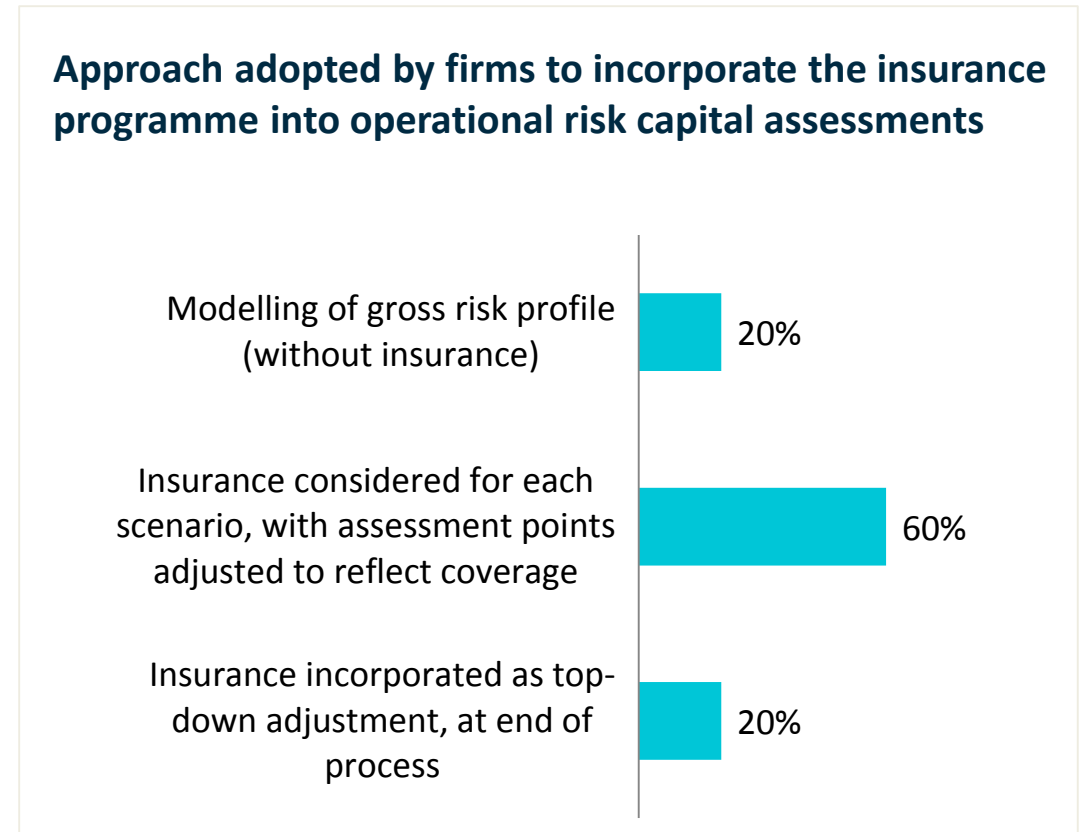
1. Aligning operational risk and insurance

State of the market (2 / 3)¹

Use of insurance for capital purposes



Approach to incorporate insurance



1. Based on survey of 25 insurers conducted during Q4 2017.

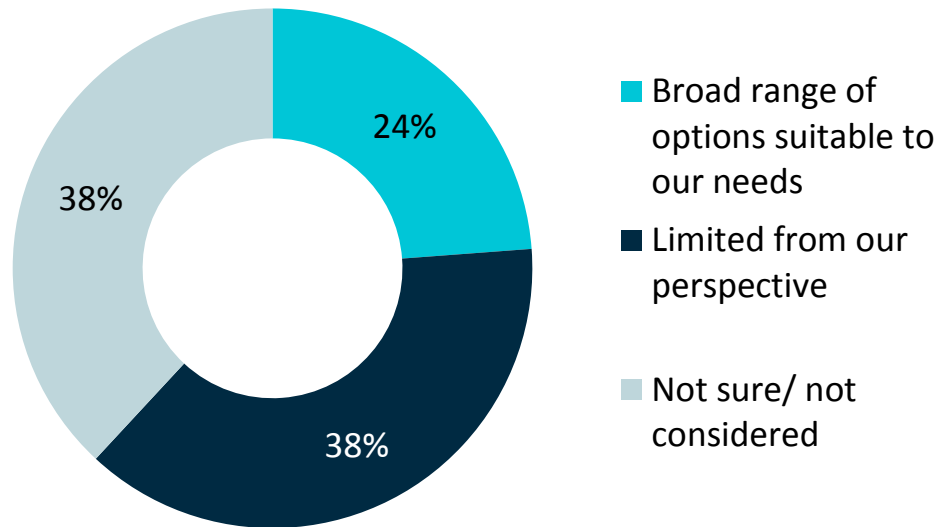


1. Aligning operational risk and insurance

State of the market (3 / 3)¹

Views on insurance options

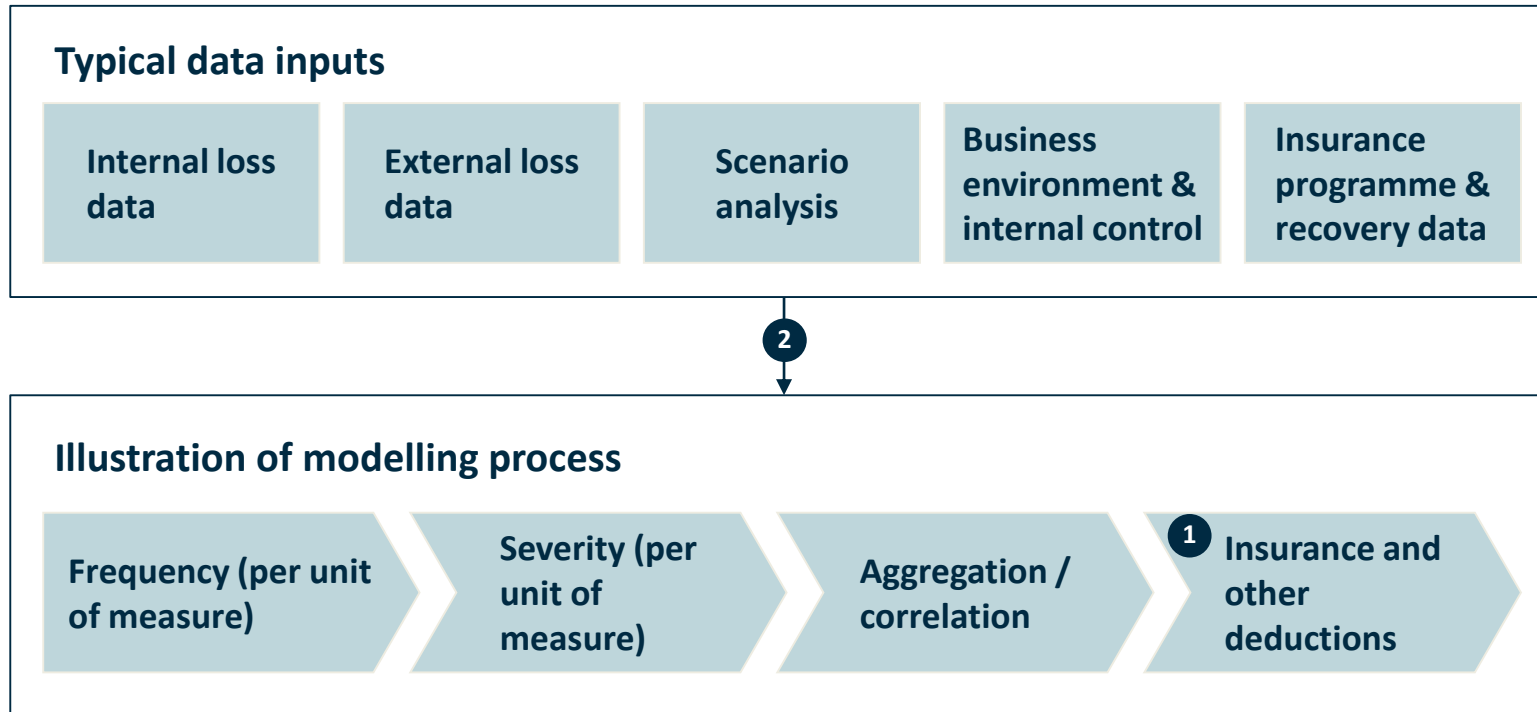
What do you think of the range of risk transfer solutions available in the market?





2. Incorporating insurance into models

Approach to incorporating insurance into models



Broad possible options

- 1 Standalone modelling of insurance recoveries
- 2 Adjustment of inputs to reflect current insurance coverage (e.g. scenario estimates)

- Should consider probability that policy will respond and apply appropriate haircuts, e.g. reflecting:
 - Credit rating of the insurance provider
 - Residual term of policy
 - Policy provided by a third party
 - Time to recover losses
- Importance of structure & data-supported approach



3. Operational risk insurance

Potential transfer options

- Both traditional and bespoke operational risk insurance can be used to transfer a firm's operational risk profile
- Bespoke operational risk policies allow for a range of potential structures to meet specific needs, e.g.:
 1. Per loss catastrophic layer insurance of major scenarios/units of measure
 2. Annual aggregate operational risk insurance across all risks (to the extent legally insurable)

What can be covered

- Potentially any Operational Risk is insurable:
 - Substantial contributor to Operational Risk capital
 - Legal to insure
 - Adequate control structure
- Examples:
 - Misselling (less disgorgement)
 - Fraud
 - Processing / execution error
 - Conduct risks
 - Cyber
 - Breach of investment mandate



3. Operational risk insurance

Operational risk insurance market

- Large capacity available
- Number of transactions in place
- Primarily for Banks and Asset Managers
- Financial Infrastructure Providers
- Increased use for non-Financial Institutions
- Growing interest among Insurance Companies

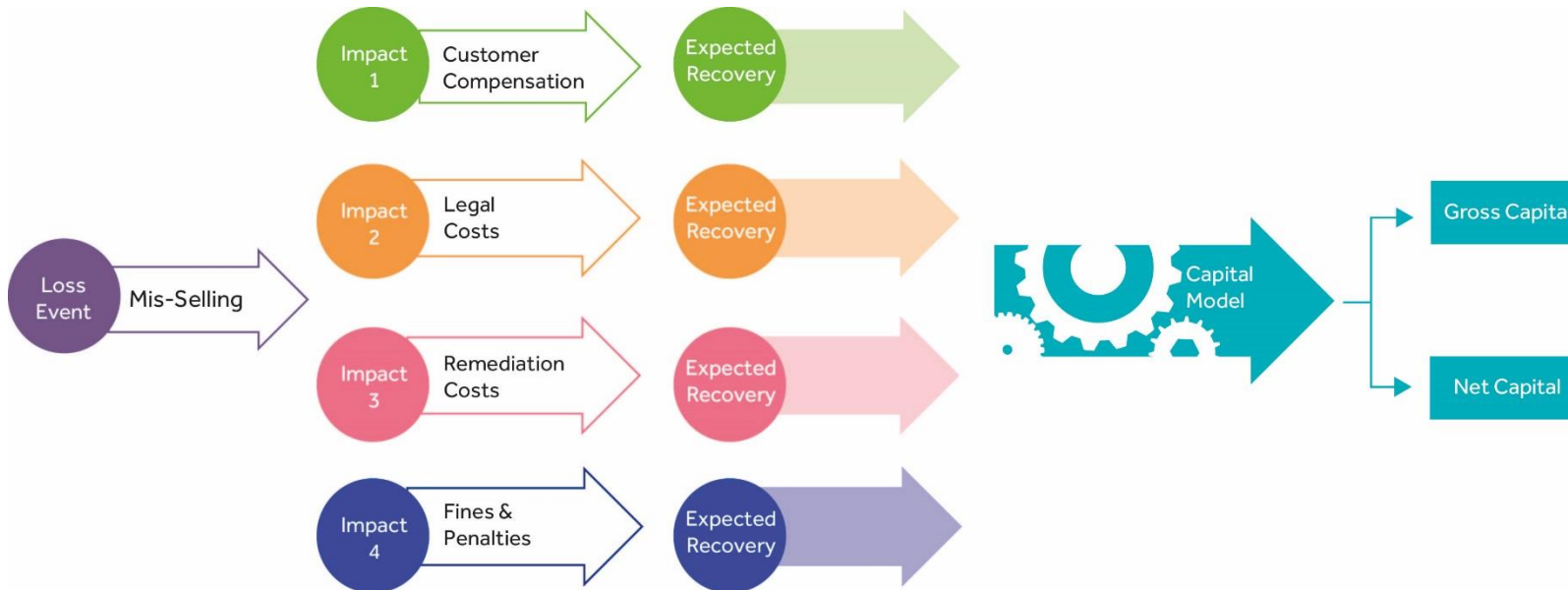
Current purchasing trends

- Larger capacity
- Focus on key risk drivers – usually scenario driven
- Confidence of response over multiple risk cover
- Increased demand for customised solutions
- Most significant challenge – internal silos
 - Programme design
 - Valuation and communication



3. Operational risk insurance

Engaging with underwriters



Benefits

- Explicit modelling of insurance recoveries
 - For each loss or scenario
- Application of deductibles and limits
 - Per loss and policy
- Confidence in performance / timeliness of payment
 - Eliminating coverage mismatch / uncertainty



3. Operational risk insurance

Underwriting process

I. Risk Identification

Prioritise significant risks

- Capital drivers
- Forward looking risk / scenario

II. Stakeholder Engagement

Joint team

- Operational Risk / ERM
- Capital Modellers
- Finance
- Risk Managers / Brokers

III. Contract Development

Joint develop contracts

- Based on risk scenarios & capital requirements
- Buying motivation
- Valuation metrics



4. Q&A

- Do you have any questions?



Society of Actuaries in Ireland

Risk Functions: Keeping Pace with Data Analytics

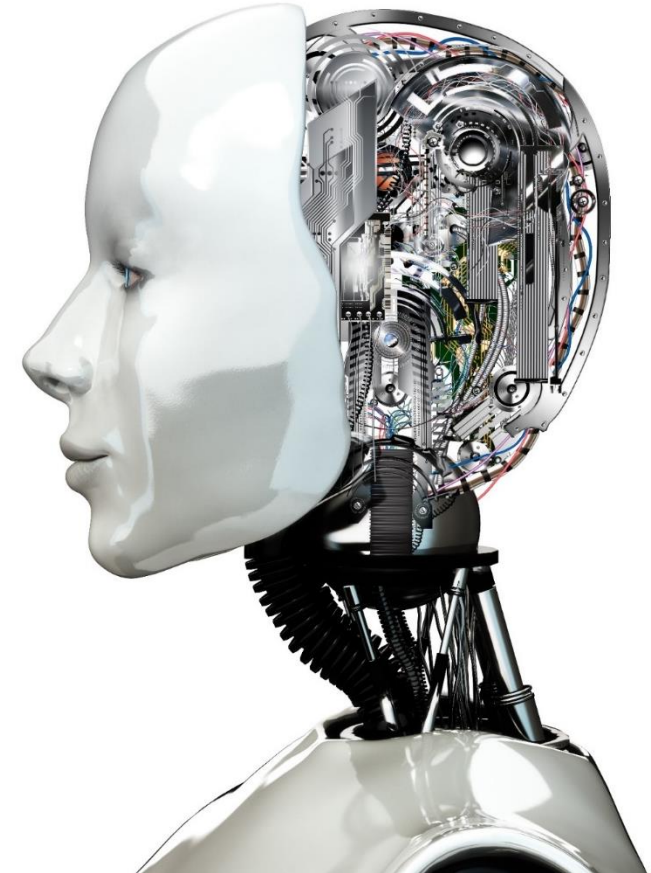
Jean Rea



Risk Functions: Keeping pace with data analytics

Jean Rea FSAI, Director, Actuarial Services

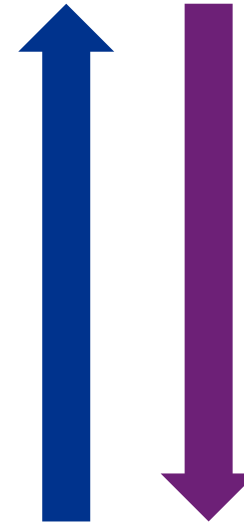
12 October 2018



KPMG CEO Outlook

The risk landscape is shifting. The risks that CEOs are most worried about have changed dramatically since 2016:

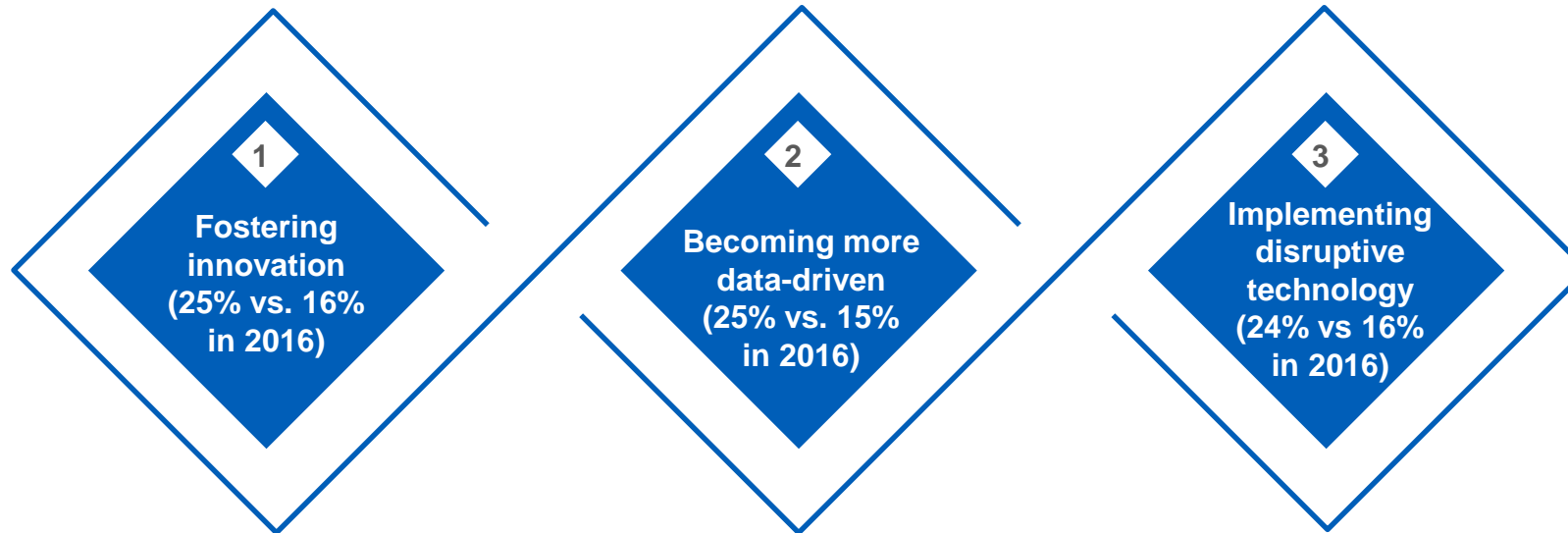
Top of mind risks	2016	2017
Emerging technologies	29%	36%
Operational risk	19%	33%
Talent	13%	27%
Cyber	42%	26%



45% And, 45% expect disruption in their sector over the next 3 years as a result of technological innovation

Strategic priorities are evolving

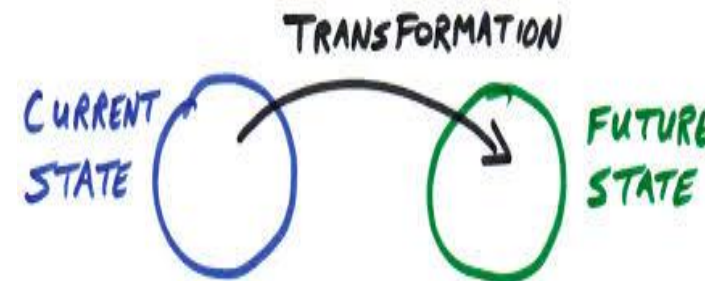
Top priorities now include:



And...

69% plan to invest into digital infrastructure over next 3 years

59% say the primary objective of their investment is to transform their business and operating models





Data



Data driven decision making Caution

Data-driven decision management (DDDM) is an approach to business governance that values decisions that can be backed up with verifiable data. The success of the data-driven approach is reliant upon the quality of the data gathered and the effectiveness of its analysis and interpretation.

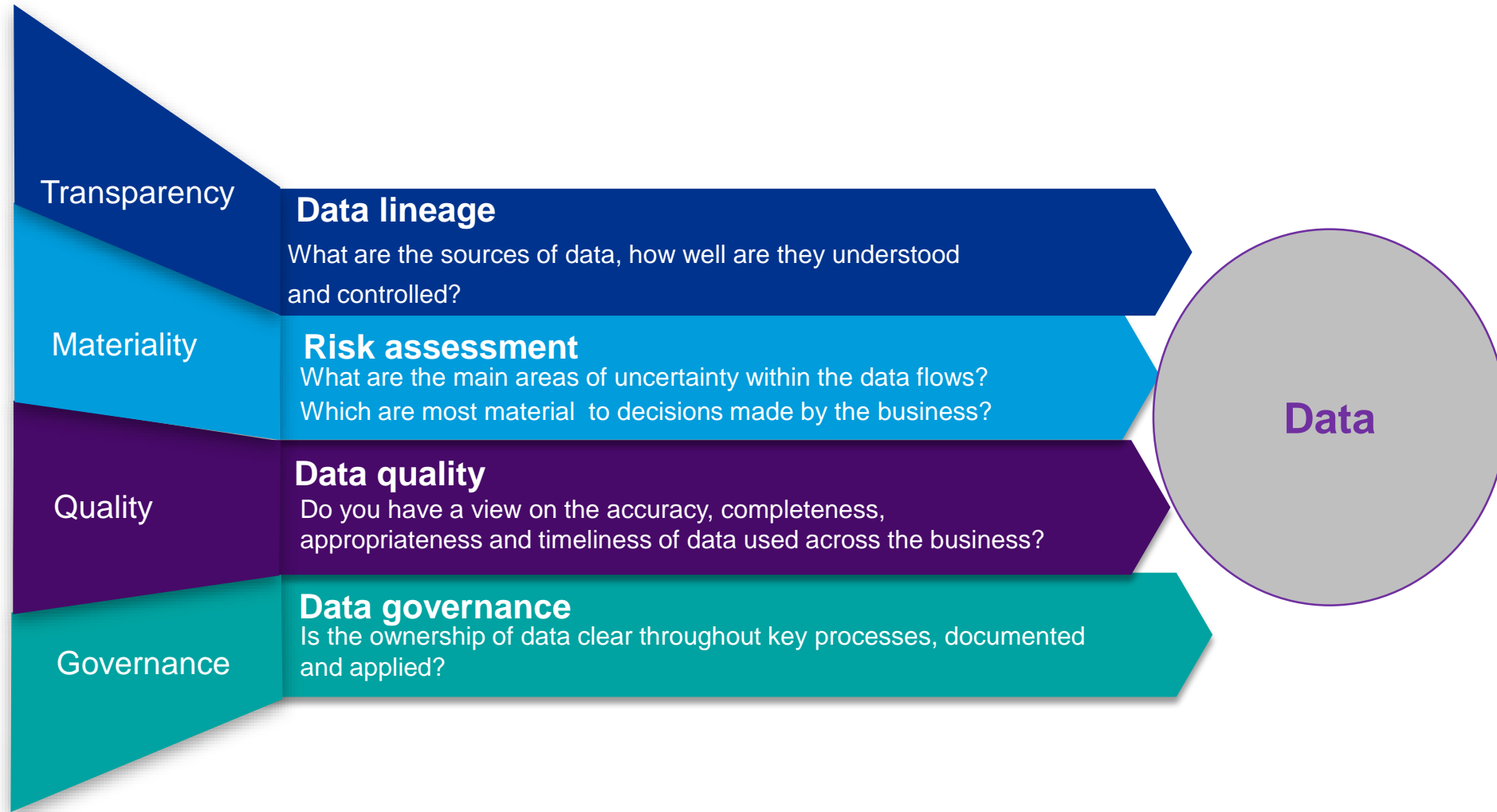
Data-driven disaster is a serious problem caused by one or more ineffective data analysis processes... The data quality may be inadequate ...

<https://whatis.techtarget.com/definition/data-driven-decision-management-DDDM>

<https://whatis.techtarget.com/definition/data-driven-disaster>

“A firm’s data is, in many cases, its biggest asset. So it is vital that firms are taking a data-centric view of their business and systems to identify what data they have or need to support their core business services, and how it is classified, used and protected....
But this can only happen if the data is reliable and available. From our on-site inspection work over the last number of years, **we have identified many weaknesses in firms’ abilities to effectively understand, use and report on their data**. Issues arise from a patchwork of legacy and newer systems that do not talk to each other, resulting in fragmented data that requires manual interventions and adjustments before it can be used. Firms need to have a **single source of their key data if they are to rely on it for critical intelligence and decision-making**. Those that manage this transition best are likely to be the firms that survive and thrive.”
Ed Sibley

Data considerations





Big data



Big Data - Consultations

Financial Conduct Authority




Feedback Statement FS16/5

**Call for Inputs on Big Data
in retail general insurance**



September 2016



29 June 2018

Industry survey - Big Data thematic review

[Information about the organisation](#)

Name of the reporting organisation:

Country:

Year in which the organisation was founded:

Total annual Gross Written Premiums (in million EUR) in 2017:

Is your organisation active in motor insurance and/or health insurance lines of business?

Does your organisation have an insurance undertaking and/or insurance intermediary license?

[Introduction](#)

[Objective](#)

On 15 March 2018 the Joint Committee of the European Supervisory Authorities (ESAs) published a report on the use of Big Data by financial institutions. The ESA's report identified a wide array of potential benefits arising from Big Data Analytics (BDA), both for the industry as well as for consumers. However, new regulatory and supervisory questions do also emerge requiring more in-depth analysis and supervisory oversight going forward.

The objective of this thematic review is therefore to find answers to some of these questions and to gather better understanding about the implications of the use of BDA in decision-making processes, business processes, emerging business models and the different stages of the insurance value chain.

[Scope](#)

The present thematic review covers the use of Big Data Analytics in motor and health insurance by (re-)insurance undertakings and intermediaries

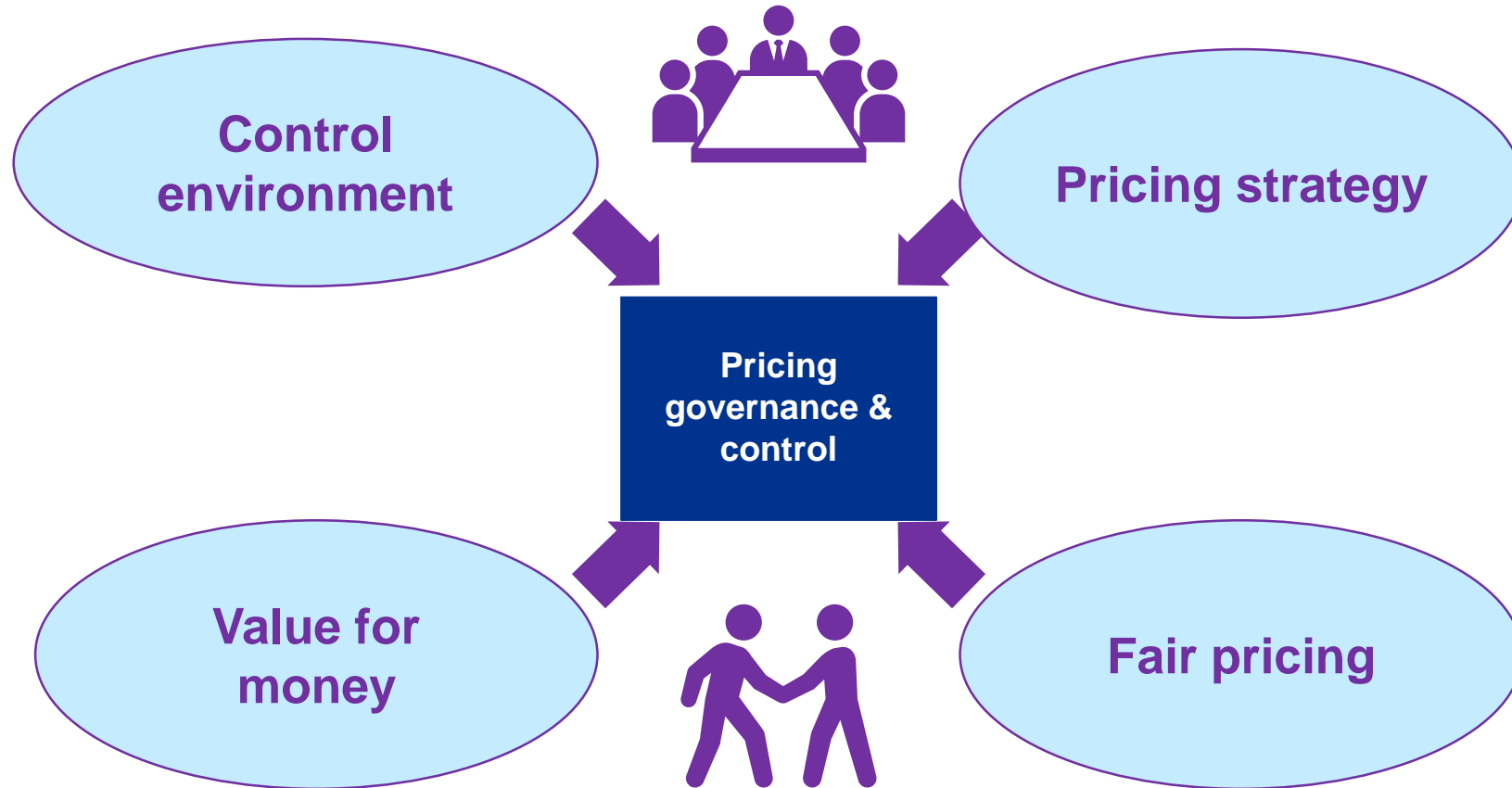
Findings in UK GI retail market

***Big Data** raises issues that range from **moral and ethical**, to how the market may develop or be constrained and **how consumer outcomes may be affected**. Many of these issues are not new in insurance, but can be **accelerated and magnified by Big Data**. In theory, some of the **outcomes for consumers** from better **prediction and segmentation** could be positive in terms of service and price. However, taken to the other extreme, it could lead to some consumers **facing difficulties in obtaining affordable insurance** or even **undermine the key concept of pooling risk**. [Source: FCA (UK Regulator), FS 16/05]*

Findings were largely positive, but the FCA did find concerns about some aspects of the impact of Big Data.

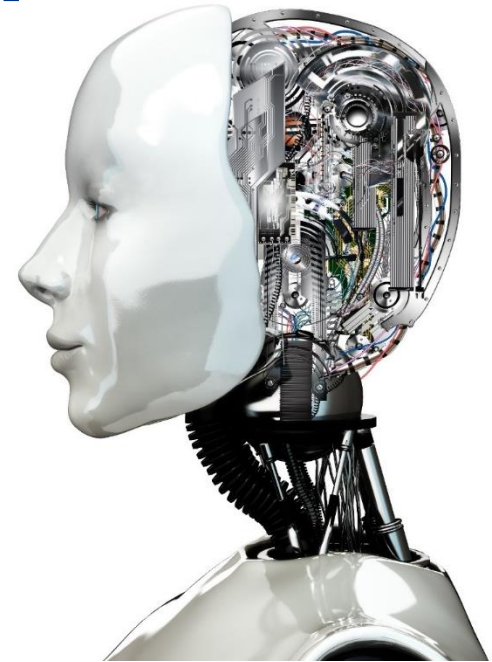
1. **Increased risk segmentation** may result in improved outcomes for some consumers, but the FCA are concerned that it could also result in **categories of consumers with higher risks that are no longer able to obtain or afford insurance for the risk they represent**.
2. **Pricing practices** Big Data may improve firms' ability to identify opportunities to charge more to certain types of customer, for example **looking at their ability and willingness to pay more i.e. not risk or cost based**. This is referred to as 'price discrimination' or 'price optimisation'. It is a common feature in many industries, but can lead to poor consumer outcomes in some circumstances.

Risk Function considerations

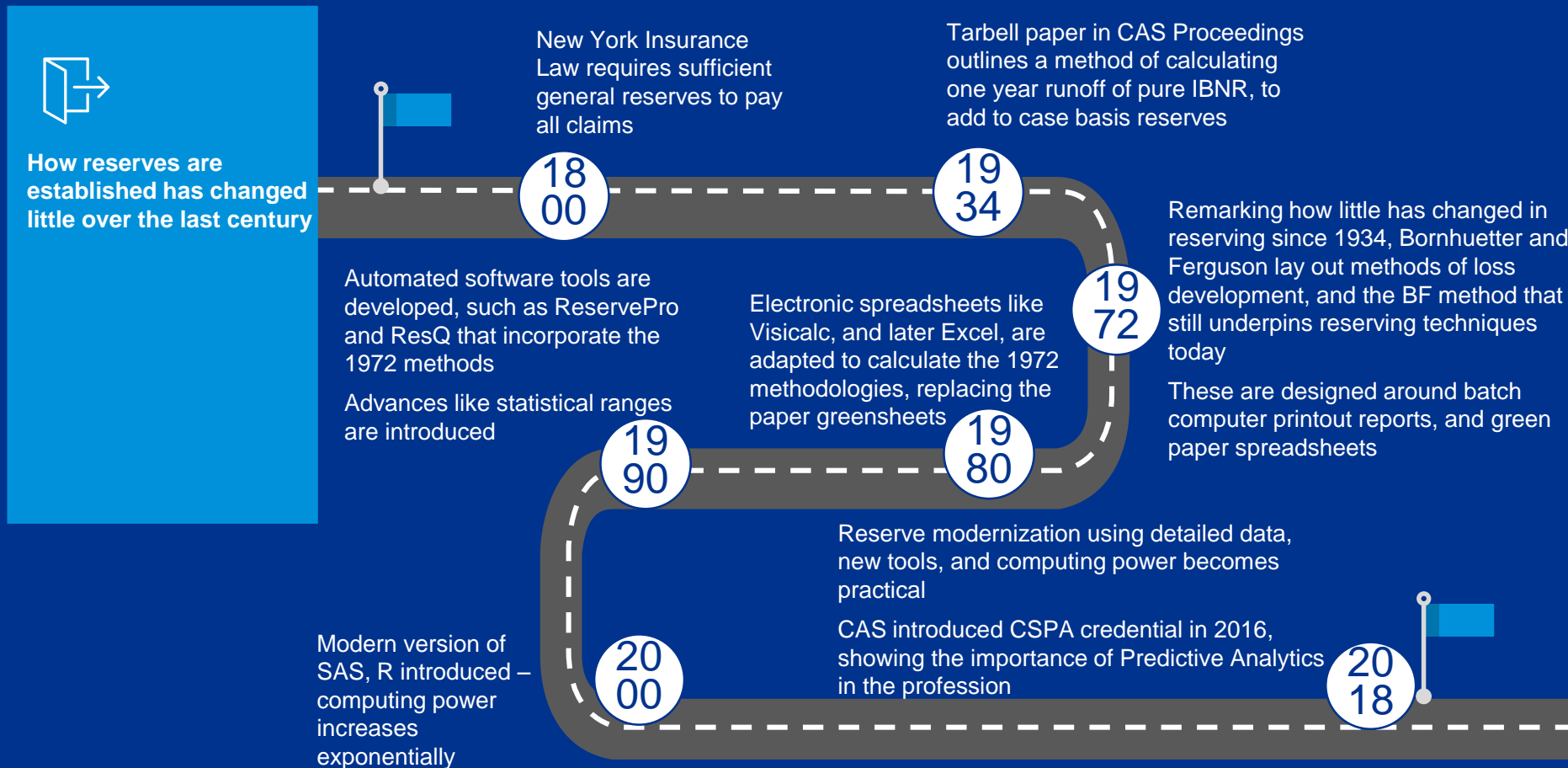




Data analytics – never mind the size, what are you doing with it?



A brief history of non-life reserving

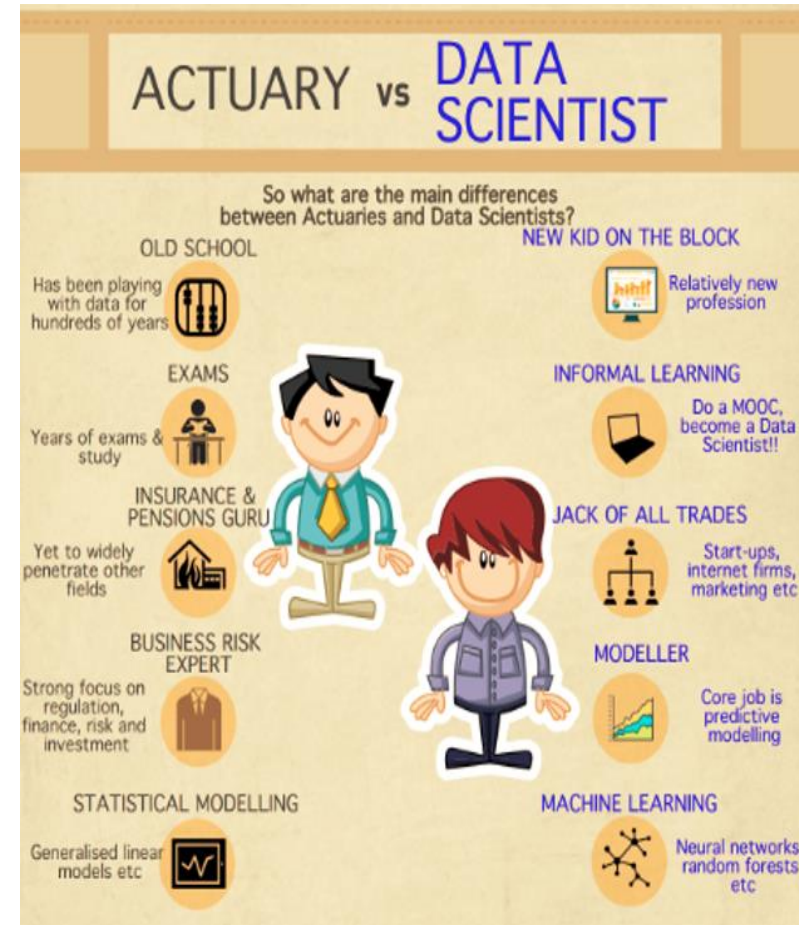
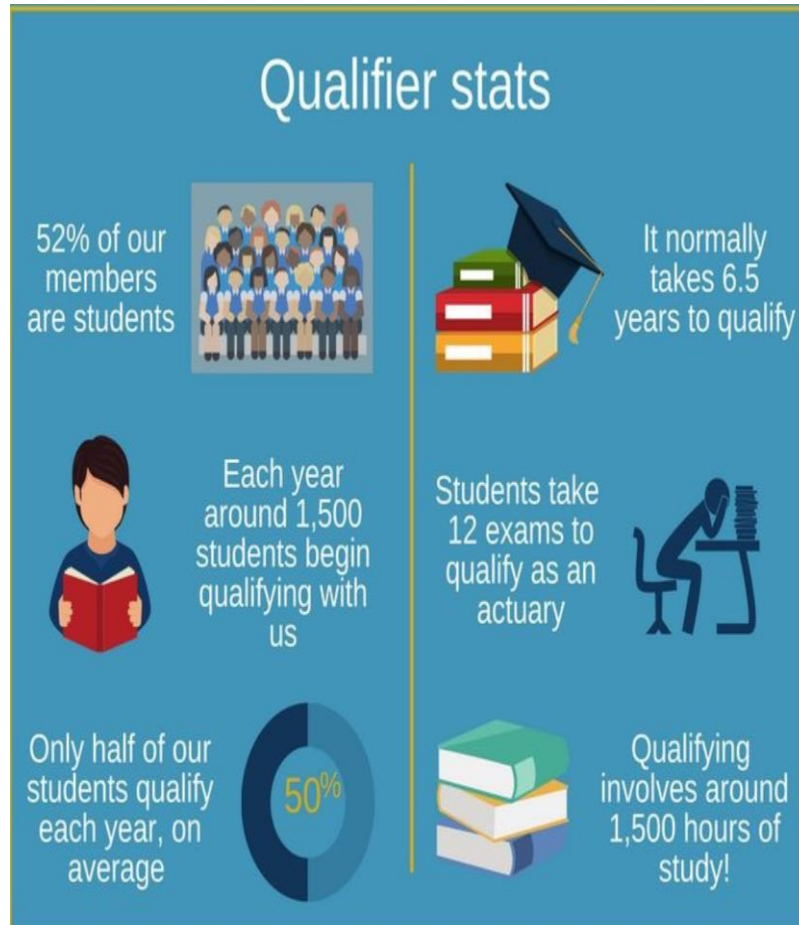


Skills

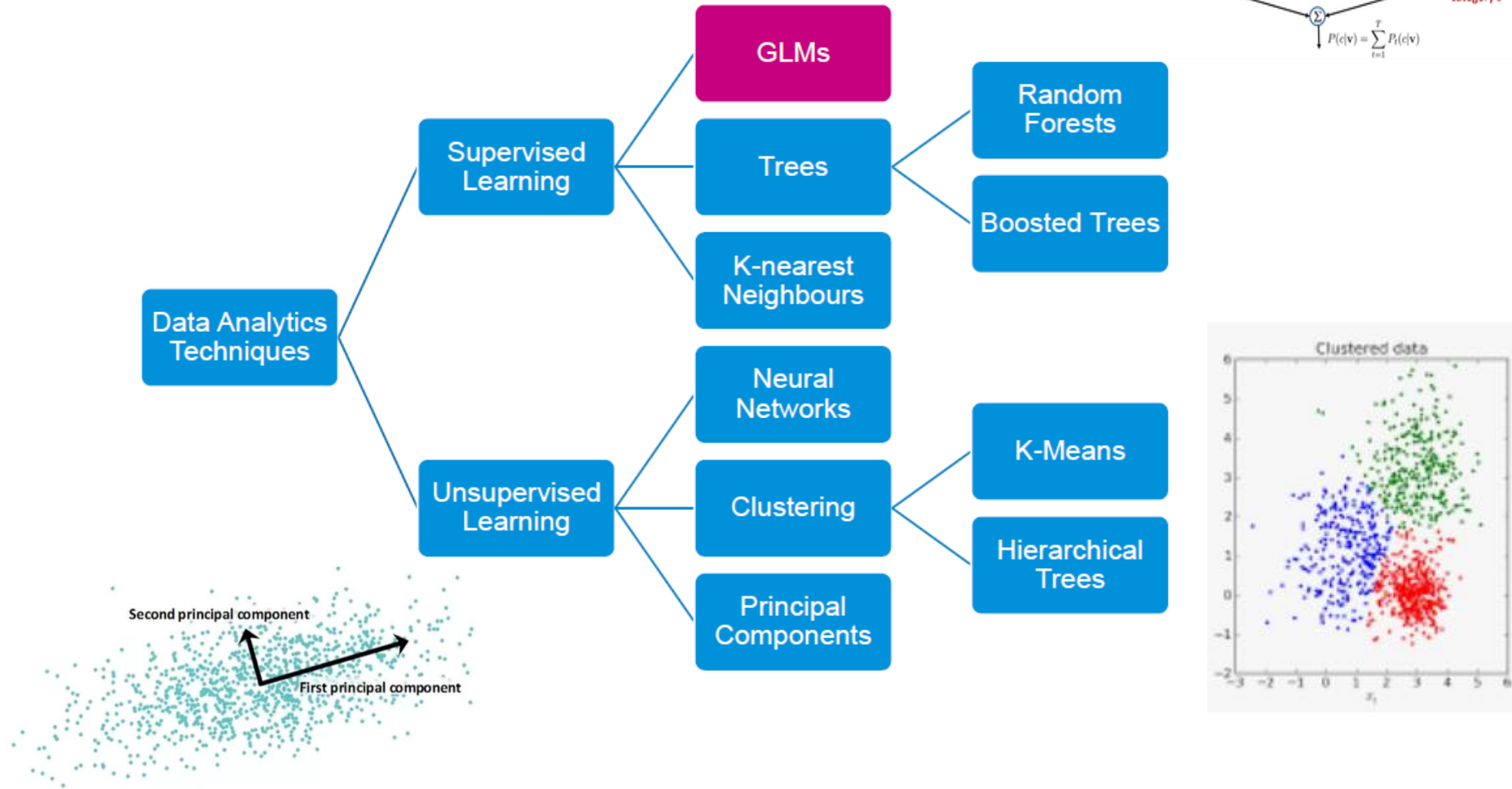


Josh Wills @josh_wills · 3 May 2012

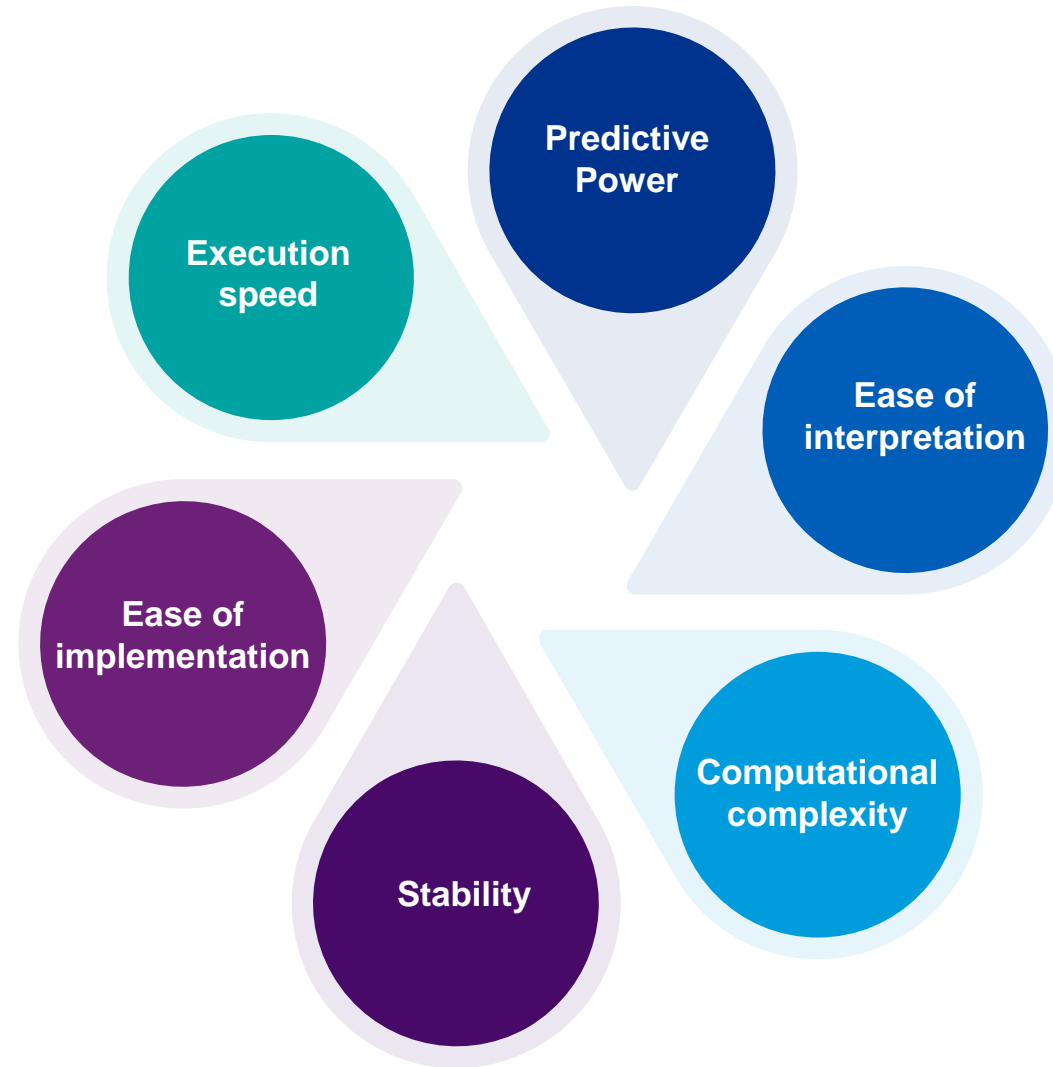
Data Scientist (n.): Person who is better at statistics than any software engineer and better at software engineering than any statistician.



Techniques



Modelling considerations



Potential benefits

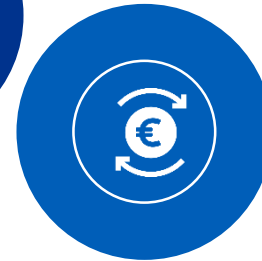
Seamless
communication



Granular Data



Faster
reaction



Increased
efficiency



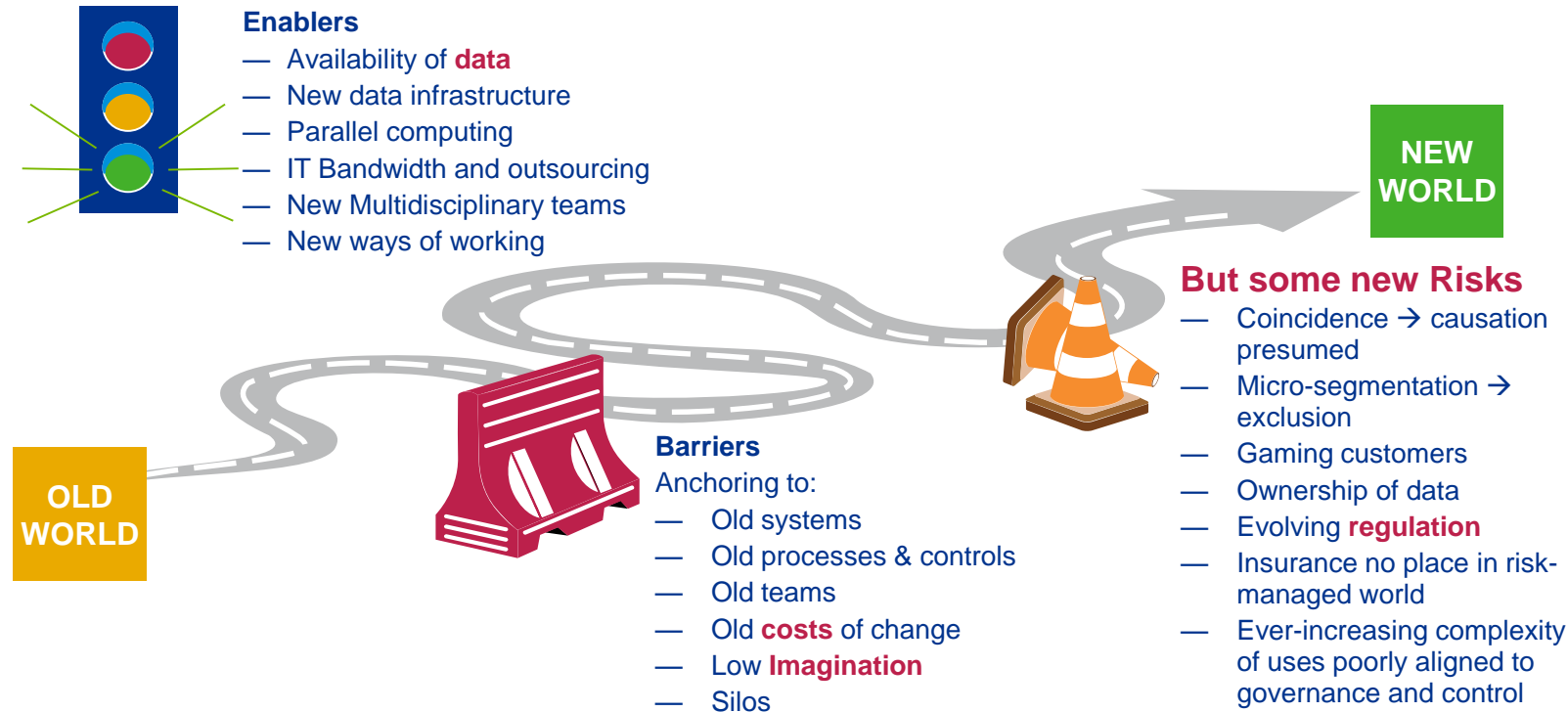
Deeper and
quicker
insight



Frequency
of review



...significant barriers remain presenting new Risks

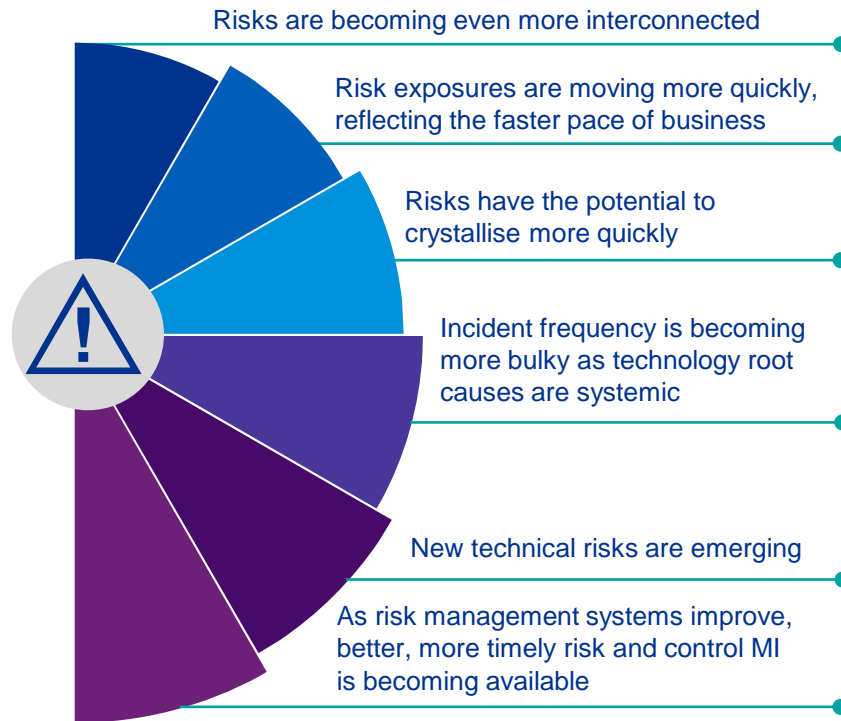




Last but not
least the
Risk
Function
itself



Digital developments further cause risks to be dynamic and interconnected



How will the tools and techniques used to assess and monitor risks change in a more connected world?

What capabilities are needed within insurers and within risk functions to manage and oversee a more connected world?

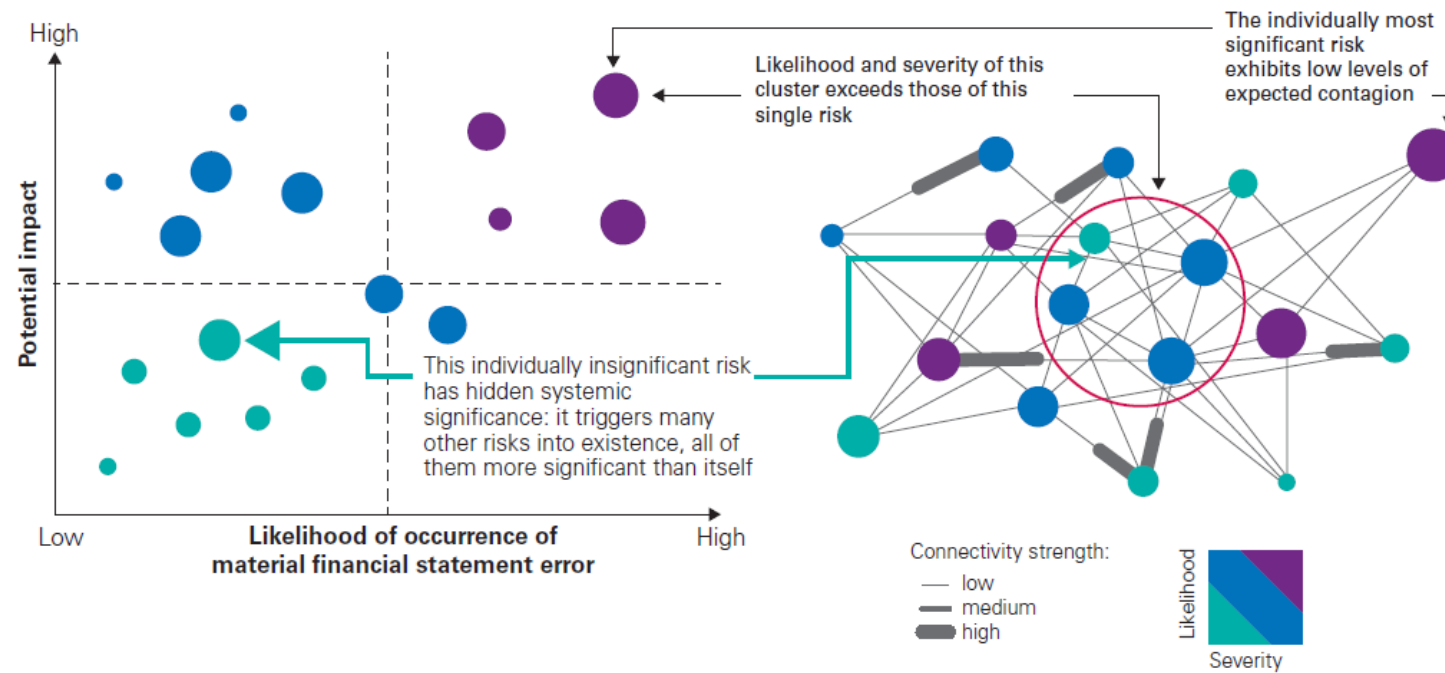
What can we learn from other parts of the business that are also impacted by changing landscapes?

...In a digital world, higher emphasis will be placed on the management of connected risks

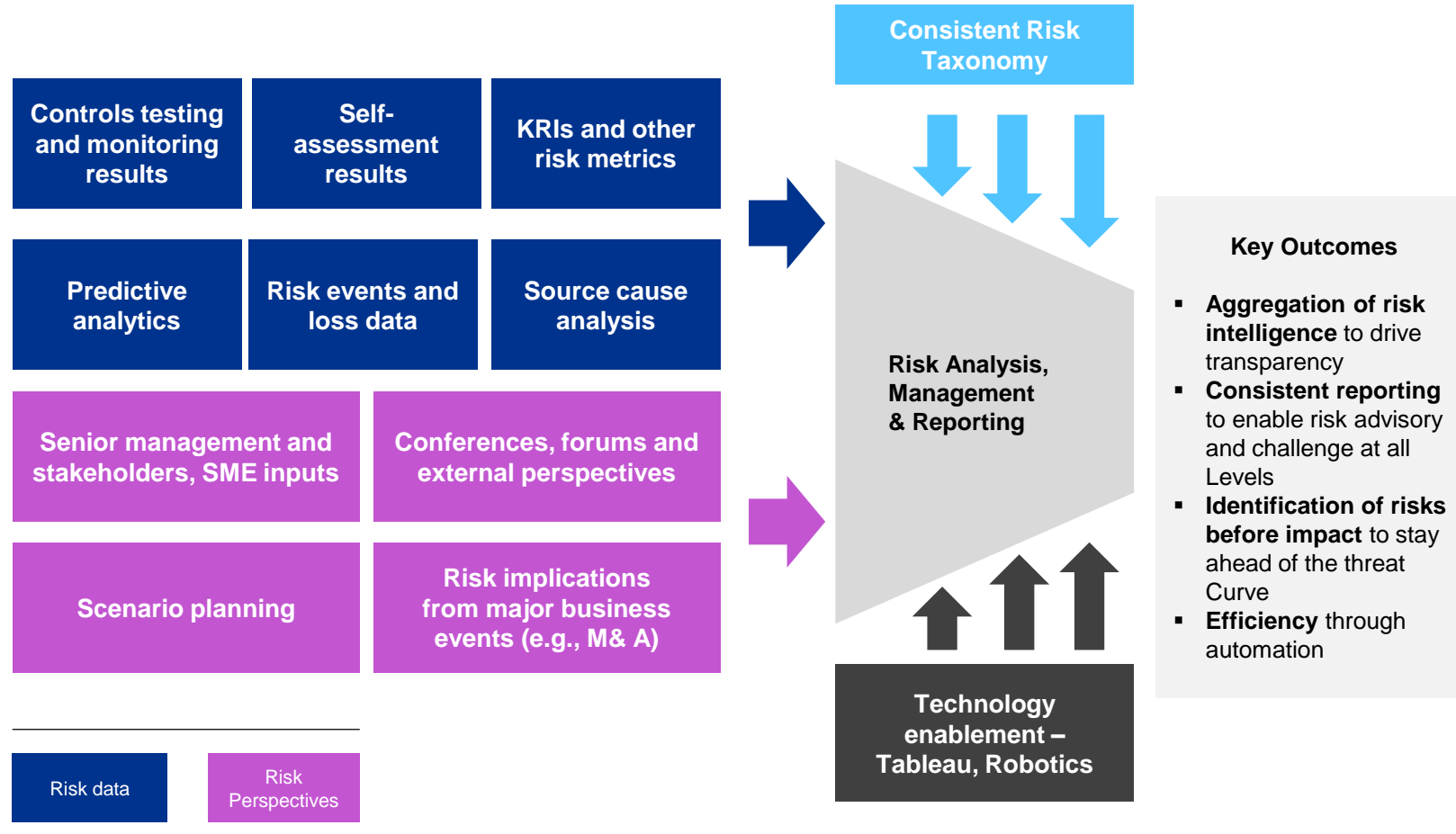
Dynamic risk assessment

Traditional, two dimensional risk map

Inter-connected view



Automated risk reporting





Any
questions?

Thank you



Society of Actuaries in Ireland

**Reliance the Board places on the Risk
Team to prepare a good ORSA**

Brenda Dunne

My background

- INED – 5 years
 - 4 Companies
 - All Life Assurance / Reinsurance companies
 - All subsidiaries of large multinational groups
- Actuary – 29 years

Agenda

- What the board really wants!
- Reliance the Board places on the Risk Team
- What makes a good ORSA ?
- Final thoughts



The Board wants

- Strategy and Capital are aligned
- Know our Key Risks
- Prevent major failure
- Trust the results



Reliance on the Risk Team - CRO

CRO is a key management and governance role

- Strong calibre
- Empowered
- Engaged with the business
- Challenging
- Resilient
- Excellent communicator
- Expert



Reliance on the Risk Team

- Multi-discipline
- Embedded in the business
- Think outside the box
- Risk mitigation
- Work closely with Finance & Actuarial
- Strong process / reliable results



A good ORSA should

- Provoke discussion
- Test our strategy and business plans
- Have good involvement from 1st line
- Improve everyone's understanding of key risks
- Enable the Board to set appropriate Capital levels
- Take account of Group views



A good ORSA should Provoke discussion

- Debate and Challenge is good!
- A continuous process – a journey not just a document
- CRO should not produce “the answer”
- Requires frequent discussion at Board
 - Standing agenda item
 - Perhaps a “workshop”
 - Board discusses stresses and scenarios
 - Brainstorm key risks
 - Early visibility of base and stress scenario results
 - Flexibility and time for “what if’s?” and reruns



A good ORSA should Test strategy & Plans

- Strategy focus on top line and bottom line growth
- Capital can be an enabler or a constraint
 - How does the business generate capital?
 - How does the business use capital?
- ORSA should clearly show capital impact of plans
 - Sales
 - Products
 - New ventures
 - Contribution from in force
 - Under base case and stress scenarios



A good ORSA should Involve 1st Line

- Identify the risks
- Manage & mitigate
- Escalate
- Promote strong risk culture
- Understand risk limits



A good ORSA should Aid understanding of Key Risks

- We have previously set our Risk Appetite
- Is it still appropriate?
- Reliance on strong ERM embedded in the business.
- What new risks are emerging?
- What risks are reducing?
- Understand our tolerance for risk
 - What are the implications of operating at the limit of our risk appetite?
 - Is there scope to accept more risk? Or should we reduce risk?
 - Where possible assign capital to risks



A good ORSA should Help set Capital Levels

- Key outcome from ORSA
- Set Target capital & Capital range
 - e.g. our target capital is 140% SCR
 - we will accept a capital range of 130% - 150%
 - Set the range based on “1in 10” or “1 in 25” year stresses
 - Consider volatility of past experience
- Inform realistic dividend expectations
 - We will only pay a dividend if we are above our target capital rangeOR
 - We will never pay a dividend which brings us below our target capital



A good ORSA should Help set Capital Levels cont.

- An additional capital buffer to protect against specific risks
 - e.g. we will hold capital of 140% SCR plus €Xm
 - we will operate at a higher capital range in the short term because of certain risks
- What happens if capital falls below acceptable range?
 - Identify trigger points for action



Possible Capital Framework

Solvency Ratio

Risk Appetite Range

150% +

Above Target

130% - 150%

Target Range

120% - 130%

Management Response

110% - 120%

Board Escalation

100% - 110%

Execute actions!

below 100%

Regulatory Intervention

below MCR

Authorization Withdrawn



A good ORSA should Take account of Group Views

- Group ORSA often required
- Group tolerances for risk likely to be higher
- Appropriate scenarios for Group may differ from ours
- Uniform report structure may be required
- Group may have formal or informal capital support frameworks
- Often a source of expertise



A good ORSA should Take account of Group Views

- Our focus must remain on our entity
- Understand the Groups key risks
- Correlation with our Key risks
- Availability of capital in stress conditions
- Two way communication



A word on recovery plans

- Reverse stress testing
 - Scenarios that would reduce capital below 100% SCR
 - Events that could break our business model
- What are our recovery options?
 - Capital support from Group
 - What if not available?
 - Close to new business
 - Reduce capital requirements e.g. through reinsurance
 - Dispose of blocks of business
 - ALM
 - Others?



Some final thoughts

- HoAF signoff – useful?
- Peer Review
- Performance versus base case?
- Time / effort
- ORSA “on demand”
 - Mini ORSA



Questions / Comments



Society of Actuaries in Ireland

Geopolitical Risk and Macroeconomic Update

Jim Power

‘Geopolitical Risk & Macro Economic Update’

SAI Risk Management Perspectives Conference

October 12th 2018



Jim Power
economics

International Economic Context

- 2017 a great year, 2018 not quite as great, but
- Global economic cycle still solid
- Labour markets improving
- Inflation well behaved when energy is excluded
- Interest rate cycles normalising in US & UK, not yet in Euro Zone
- Equity markets still doing remarkably well
- Bond yields have not risen much
- Some emerging market stress eg: Turkey, Argentina & Venezuela

Global Growth Forecasts

	2017	2018f	2019f
World	3.6%	3.7%	3.7%
Euro Area	2.5%	2.0%	1.9%
-Germany	2.5%	1.9%	1.8%
-France	2.3%	1.6%	1.8%
-Italy	1.6%	1.2%	1.1%
UK	1.7%	1.3%	1.2%
US	2.2%	2.9%	2.7%
China	6.9%	6.7%	6.4%
India	6.7%	7.6%	7.4%

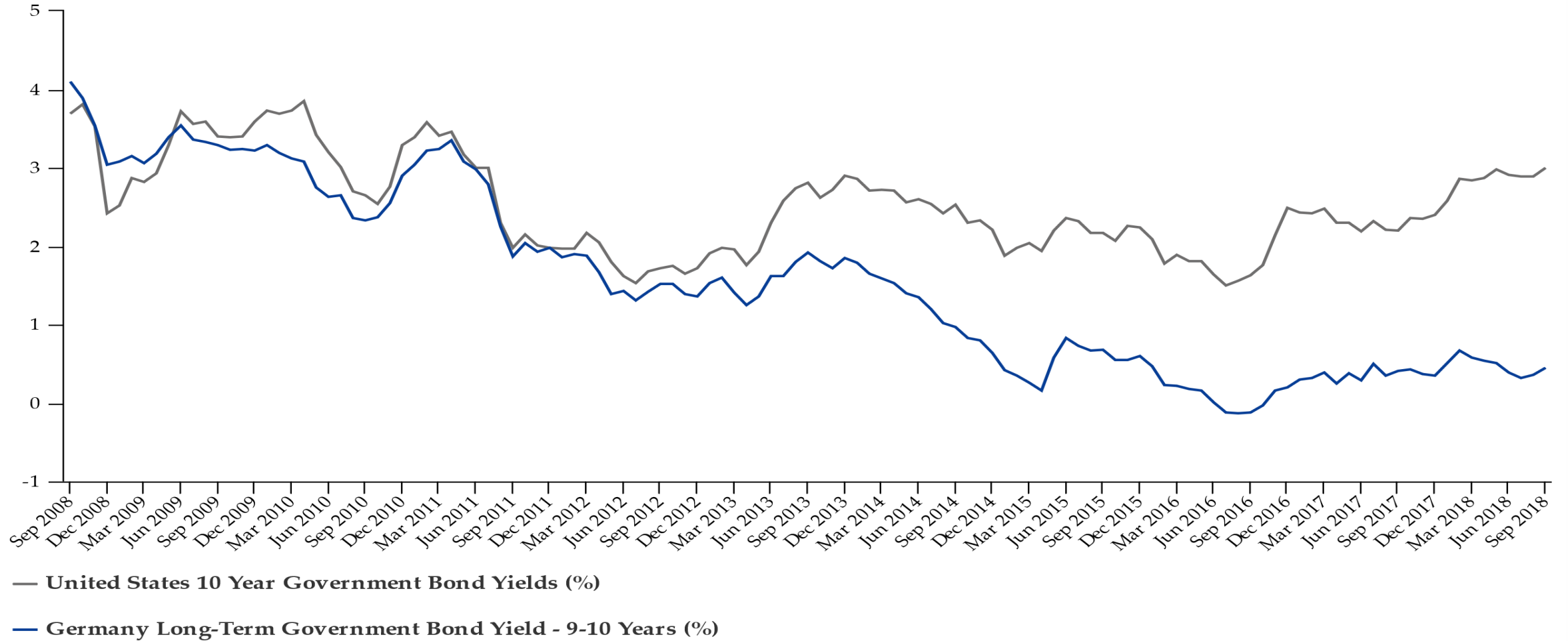
Economic Health Check

	Inflation (YoY)	Unemployment
Euro Zone	+2.1% (1.3% Ex-Energy)	8.1%
Germany	+1.9%	3.4%
France	+2.6%	9.3%
Italy	+1.6%	9.7%
Spain	+2.2%	15.2%
Netherlands	+2.1%	3.9%
Greece	+0.9%	19.1%
Portugal	+1.3%	6.8%
Ireland	+0.9%	5.4%
UK	+2.5%	4.0%
US	+2.7%	3.7%

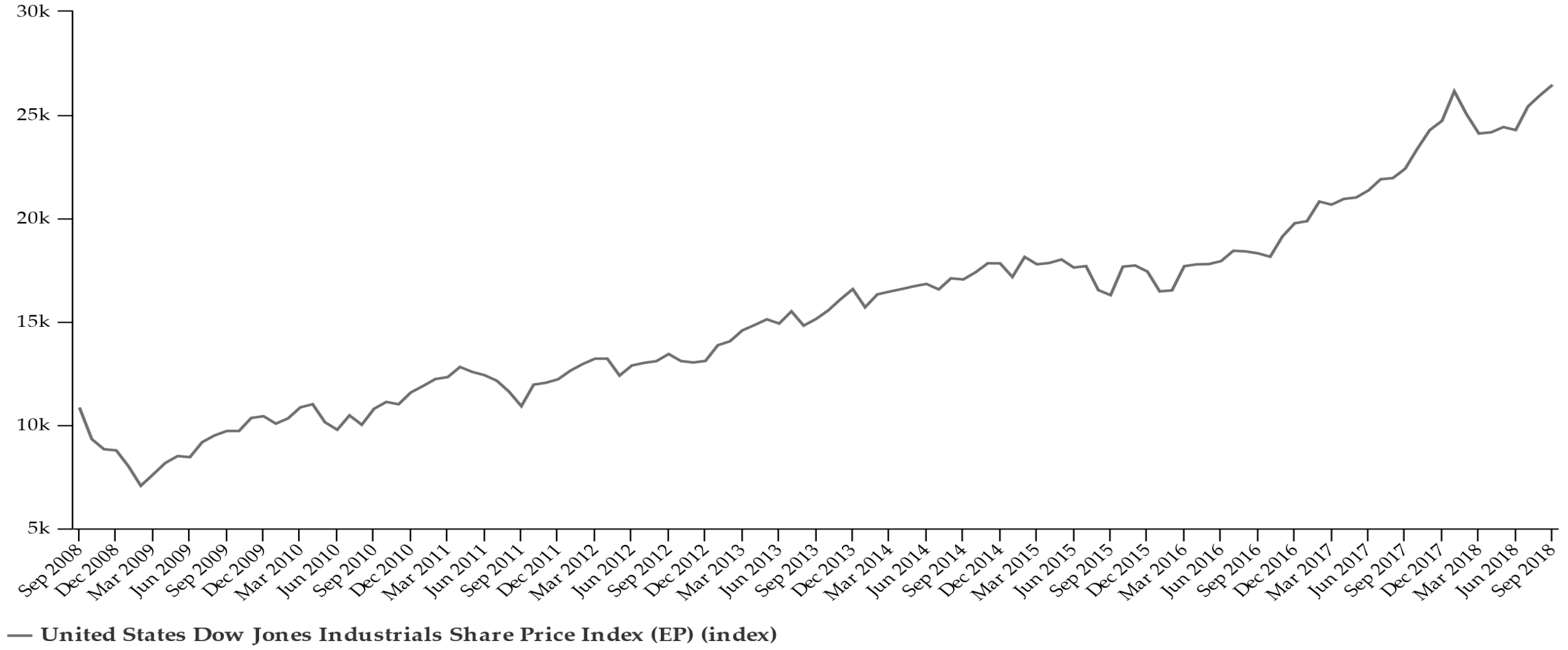
Interest Rates

- Inflation has been muted in most parts of developed world, but some pressures emerging
- US Fed Funds up from 0% to 2.25% since Dec 15 > another 1% over coming year
- UK Base Rate 0.75%– limited upside potential
- ECB QE from €30 bln p/m to €15 bln in Sept – will end in December
- ECB relaxed > no pressure for the moment, but risk of change later in 2019
- What is upside potential in Euro Area? 2% by end 2021?

10-Year Bond Yields



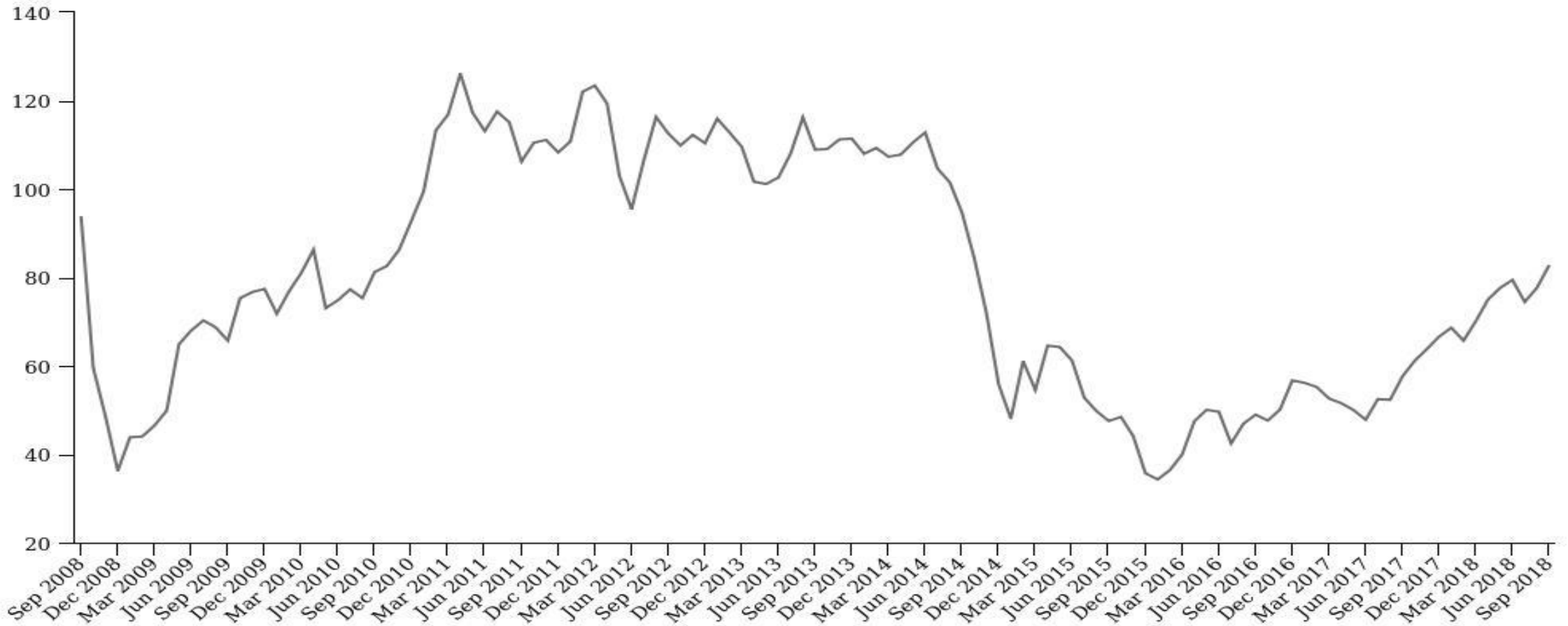
Equity Markets



— United States Dow Jones Industrials Share Price Index (EP) (index)

Sources: Thomson Reuters, Capital Economics.

Oil Prices



— Global (Commodities) Brent Crude Oil Price (USD/BBL)

Sources: Thomson Reuters, Capital Economics.

Sterling/Euro Exchange Rate



— United Kingdom UK Pound Sterling to Euro (Level)

Government Debt End-2017(% GDP)

COUNTRY	Debt % GDP
Euro Zone	86.7%
Germany	64.1%
France	97.0%
Italy	131.8%
Greece	178.6%
Spain	98.3%
Portugal	125.7%
Netherlands	56.7%
Belgium	103.1%
Ireland	68.0% (111% GNI*)
UK	87.7%
United States	105.4%

Implications of High Government Debt

- Cyclical component will be improved by growth
- When combined with demographics, will put serious pressure on fiscal policy
- Strong control over Government expenditure
- Public services under pressure
- Maximise tax revenues
- Focus attention on corporate behaviour
- Will limit ability to deal with next downturn

Global Risks

- Fiscal stimulus in US will run out of steam
- Rising US interest rates
- Trade tensions
- Global equity markets in historically long cycle
- Brexit
- Corporate debt
- High levels of Government debt
- Emerging market fears
- Rise of the right in Europe
- Global geo-political tensions
- How to deal with next downturn?

**Thank you.
Any Questions?**



Jim Power
economics

+353 1 499 0097
info@jimpowereconomics.ie



Society of Actuaries in Ireland

**Cyber Risk Scenarios for Insurance
Companies - IFoA Working Party Update**

Patrick Meghen



Institute
and Faculty
of Actuaries

Cyber Operational Risk Scenarios for Insurance Companies

Patrick Meghen, Milliman

Agenda

1) Cyber Risk Investigation Working Party

- Aims, Membership and recent paper

2) Overview

- Cyber Insurance Losses
- Attacker Motivations
- Threat Vectors
- Operational Risk Landscape

3) Building a Framework

- Building Scenarios and Framework
- Main Learning Outcomes

4) Outputs Discussion

- Summary of Results
- Controls (NIST) Assessment
- Could Cyber sit under a rule of thumb?



Cyber Risk Investigation Working Party

*The purpose of the working party's research is to provide insight for actuaries working on **capital requirements** for insurers setting out the **potential impact of cyber risk events** and the **measures available to mitigate this risk**.*

The aim is to create a greater awareness of the risks for insurers, and highlight emerging issues in an area that is changing rapidly as the dependency on computer systems to support insurer's business increases.

1) Actuaries



2) Cyber experts



3) Academics



Institute
and Faculty
of Actuaries

Sessional Paper



Institute
and Faculty
of Actuaries

Cyber operational risk scenarios for insurance companies

Research project

By the Institute and Faculty of Actuaries' Cyber Risk
Investigation Working Party

Presented to the Institute & Faculty of Actuaries



Institute
and Faculty
of Actuaries



Institute
and Faculty
of Actuaries

Overview

12 October 2018

Massive Equifax data breach hits 143 million

Home Depot to Pay \$27.25m in Latest Data Breach Settlement

Target to pay \$18.5M for 2013 data breach that affected 41 million consumers

Uber concealed massive hack that exposed data of 57m users and drivers

Facebook Security Breach Exposes Accounts of 50m users

British Airways Faces Class-Action Lawsuit Over Data Breach

Government under pressure after NHS crippled in global cyber attack as chaos looms

Threat Actors (& Attacker Motivations)

Serious Organised Crime

- Theft of PII
- Credit Card Theft
- Theft of IP
- Ransomware
- DDoS
- Corp. Espionage
- Extortion

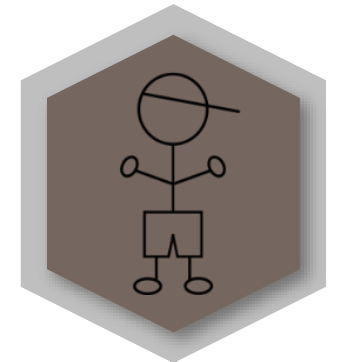


State Sponsored Group

- Theft of PII
- Theft of Secret Intelligence
- Cyber Warfare
- DDoS
- Sabotage

Extremist Groups

- Publicity
- Recruitment
- Widespread Disruption
- Espionage
- Sabotage



Opportunists / Script Kiddies

- Impress friends
- Gain credit in computer communities
- Unauthorized Entry
- DDoS



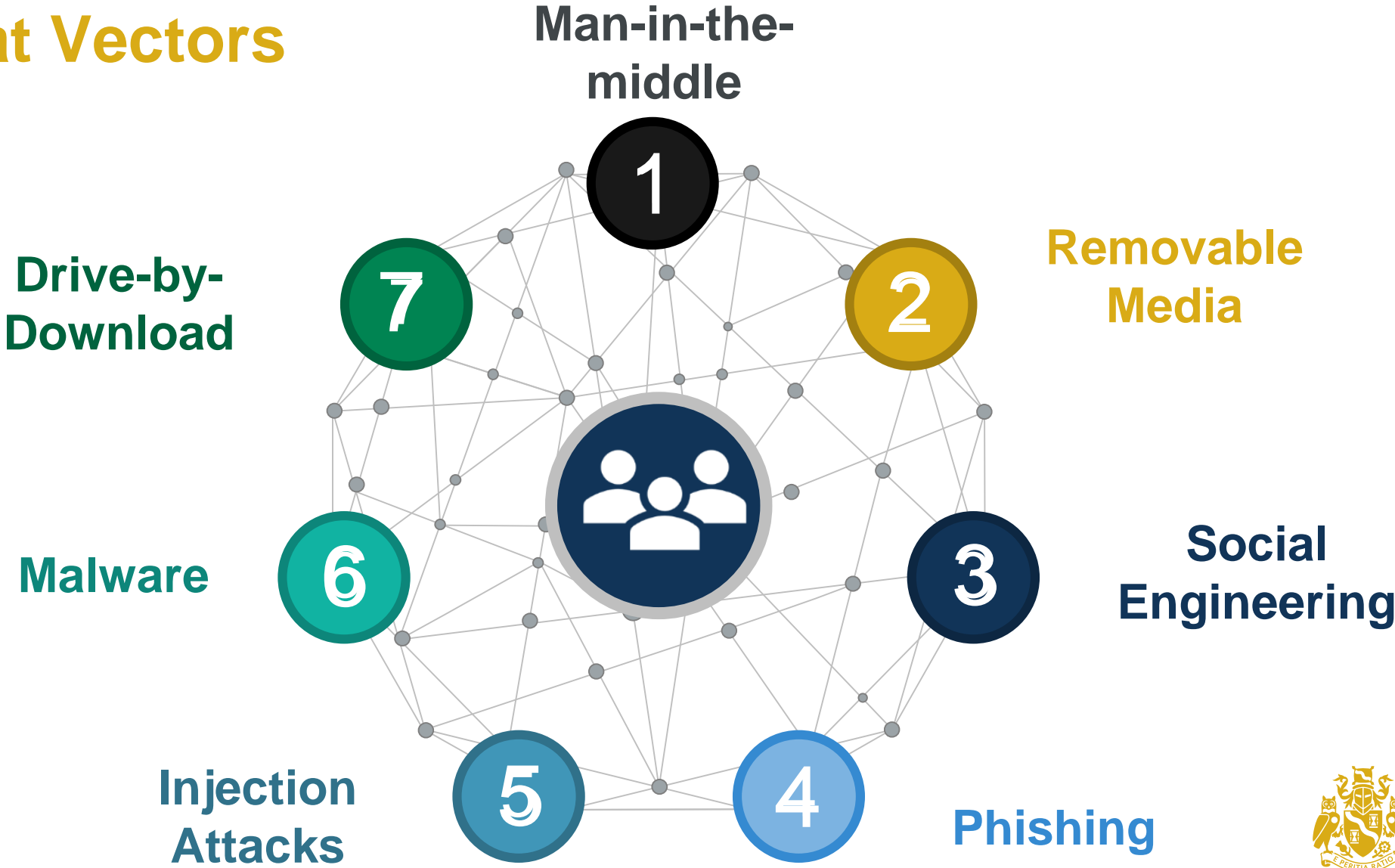
Institute and Faculty of Actuaries

Malicious Insider

- Dispute
- Vengeance
- Data Manipulation



Threat Vectors

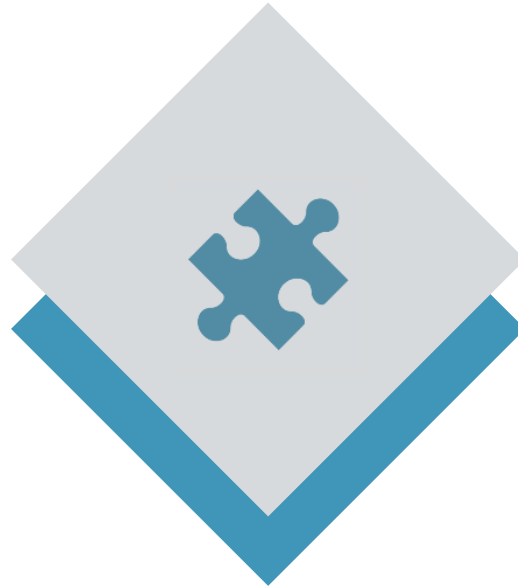


Why Cyber Risk should be assessed?



Capital Load

Cyber risk is routinely cited as one of the most important sources of operational risks facing organisations today



Risk Assessment

Actuaries need to have a robust assessment of the potential losses stemming from cyber risk, as part of an overall risk management framework



Regulation

Regulators and legislators are increasing their focus on this topic (GDPR)





Institute
and Faculty
of Actuaries

Building a Framework for Quantification

12 October 2018

Building Scenarios and Framework

1. Definition & Taxonomy

- Cyber Risk is the risk of any financial loss, disruption or negative reputational impact because of a failure in information technology systems; whether through people, process or technology.
- Common Taxonomy
 - Vulnerabilities: NIST framework (National Institute of Standards and Technology 2018)
 - Cost/Impact: CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk (CRO Forum 2016).



Building Scenarios and Framework

2. Scenarios

a) Brainstorm

- Broad range of ideas
- Involve experts within the business
- Prompt list – “Cambridge Centre for Risk Studies: Managing Cyber Insurance Accumulation Risk”

b) List of Scenarios

- Representing different types of attacks, losses, companies
- Brief description

c) Scenarios Selection

- Focus on key scenarios if limited time/resources

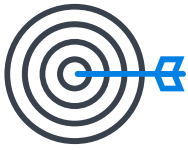


Description of Scenarios



1. General Insurer hacked by employee.

Policyholder details leaked onto Web



2. Large Life Insurer victim of spear phishing attack.

Large transfer of investment funds to rogue bank a/c



3. Lloyd's syndicate with large USA portfolio.

Cyber anarchists take down internet in East coast for 2 weeks



4. Large Insurer migrating data to cloud.

Data stored on a disk and is stolen during the transfer



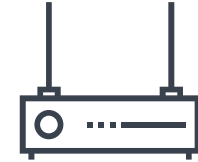
5. Ransomware spreads from a broker system to a GI system.

Major file with client records is encrypted, as is the backup



6. Third party who handles printing of statements for an insurer.

Notifies insurer they have suffered a data breach



7. How to hack a telematics device is posted online.

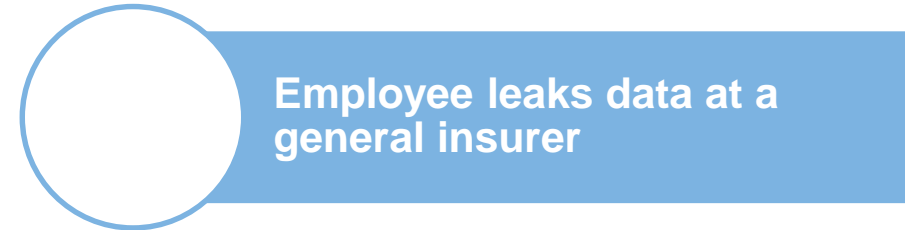
Motor Insurer must recall / replace



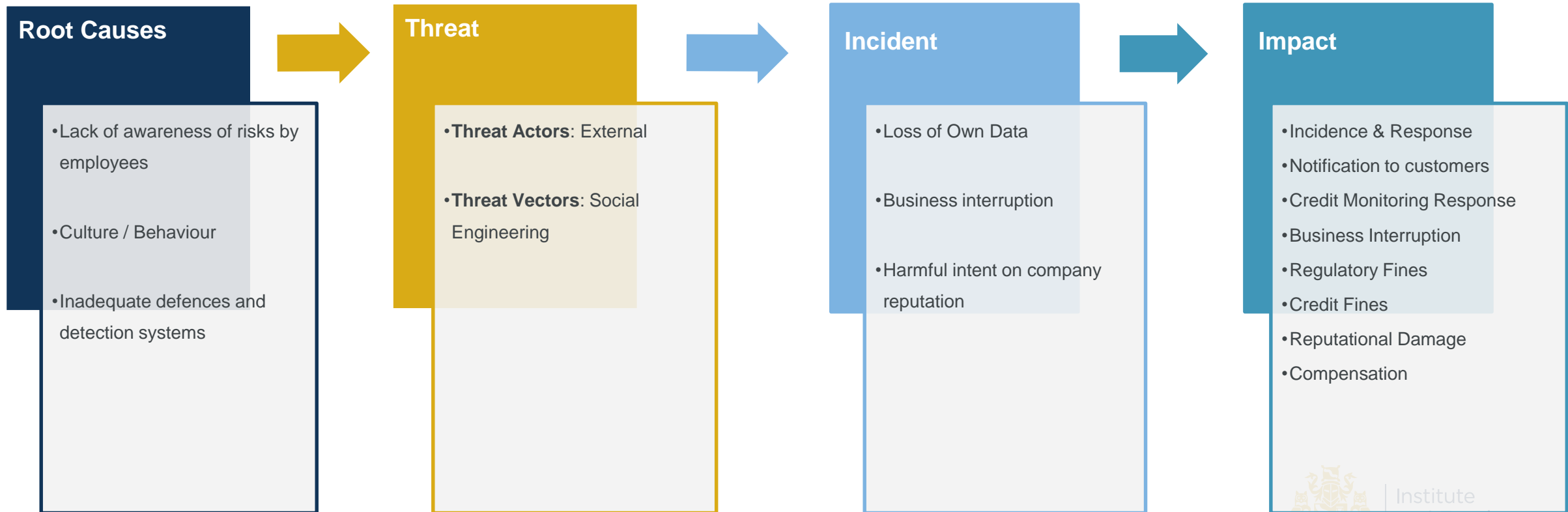
Building Scenarios and Framework

3. Further Development of Scenarios

- Why do it?
- How to build scenario that is relevant?
 - Draw on sources available e.g. CRO Forum/NIST/Threat reports
- How to build one that is quantifiable?
 - Tangible & intangible costs
- What are the most important aspects?
 - Consistency/repeatable/updatable
 - Communication
- Threat actors/vectors- how much should we care?



Building Scenarios and Framework



Building Scenarios and Framework

4. Scenario quantification

- Assessment against the NIST framework
- Costs estimation approach
- Mitigation assessment
- Consistency
- Transparency

5. Validation

- Do the scenarios make sense to experts? Use experts as often as possible!
- Actuaries cannot solve this on their own
- Breaking down language/jargon/acronym barrier, talking in the same language is difficult
- Uncertainty vs absolutes: combining two types of thought to something usable/relevant



Main Learning Outcomes

1. Build a **scenario structure/taxonomy**
2. Build a **cost structure/taxonomy**
3. Think about the **threat actors and vectors**
 - scenario should be relevant to your entity
4. Consult **Cyber/IT experts** (as many as possible)
5. Environment **rapidly changes**, be prepared to keep learning



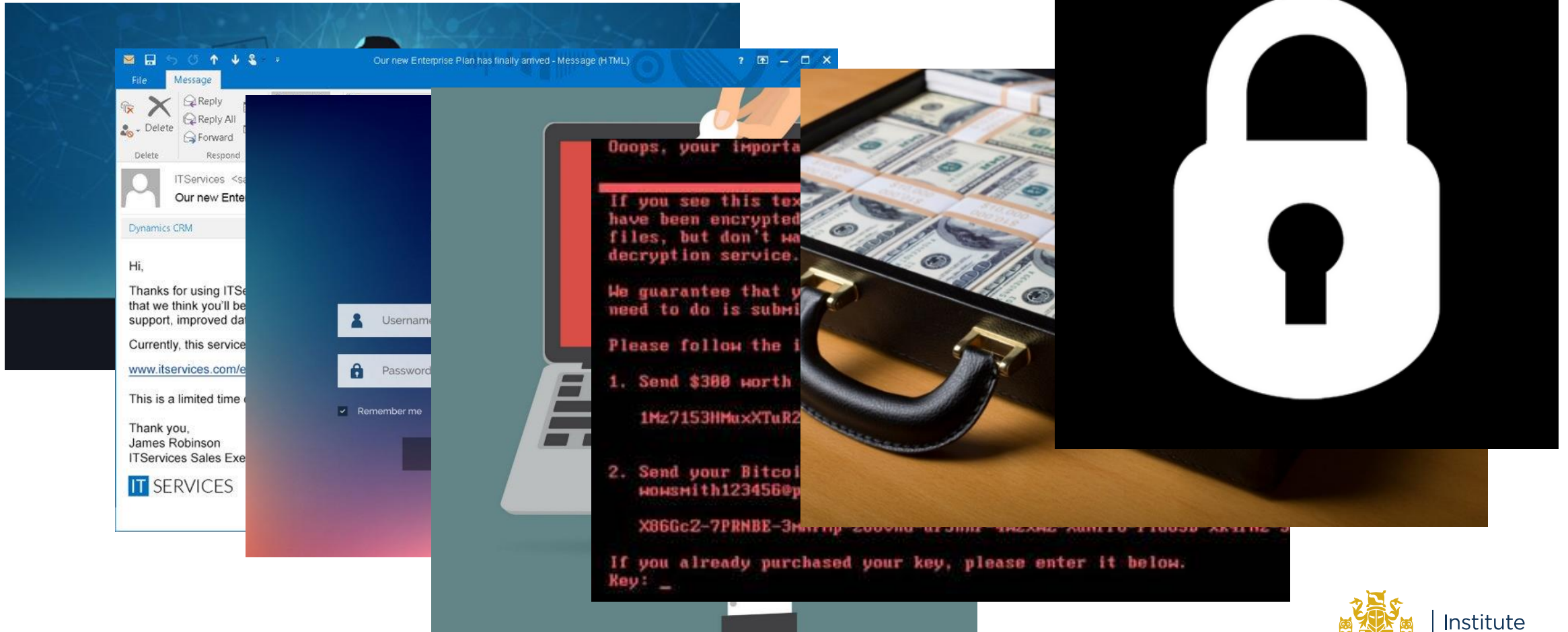


Institute
and Faculty
of Actuaries

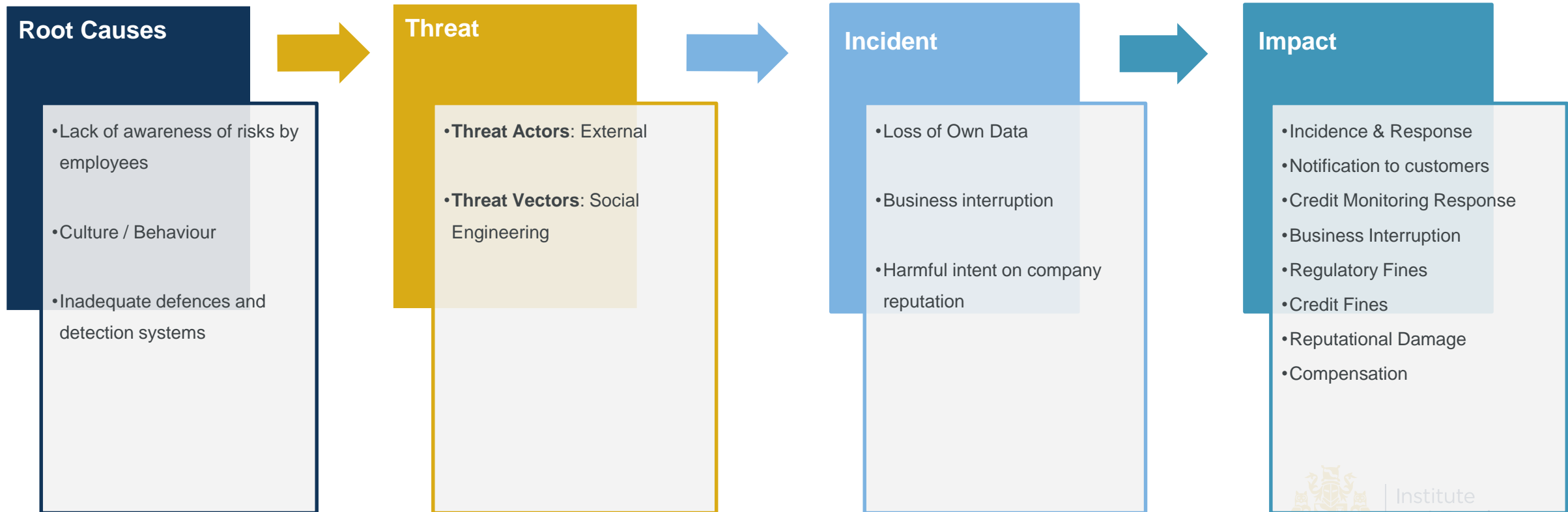
Output – detailed example

12 October 2018

Cyber extortion - narrative



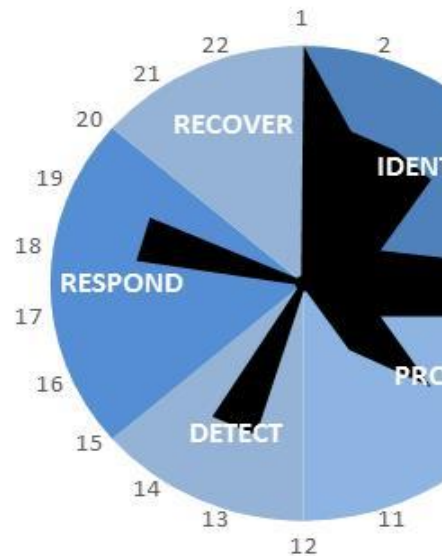
Building Scenarios and Impacts



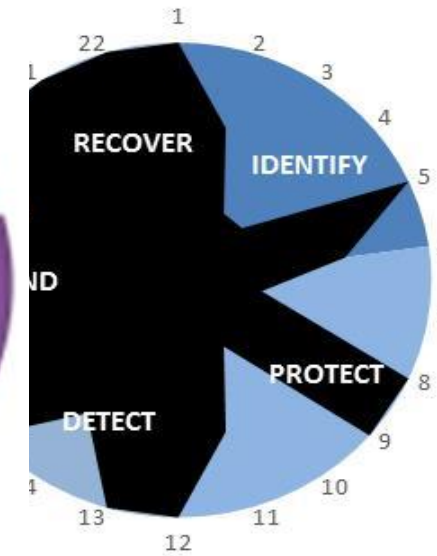
Cyber extortion scenario – NIST assessment

- Assessment of this scenario's vulnerability across the NIST framework for the impact on frequency and severity of the event

Frequency Assessment



Severity Assessment



Materiality:
 1 = Low
 2 = Medium
 3 = High



Institute
and Faculty
of Actuaries

Cyber extortion scenario – expected costs

	Cost type	Scenario cost	Approximate cost (gross)
1	Ransom Costs	Payment of ransom.	£7.5m
2	Incident response costs	IT forensics, crisis management, communications.	£1.5m
3	Data restoration	Restoration project (malware decontamination, data restoration / recreation, system rebuild).	£10.0m
4	Business interruption	Expense risk, including productivity loss due to data centre outage, transaction delays, which require rectification, unbudgeted overtime and temporary staff costs.	£33.0m
5	Business interruption	Increased liability due to delays with processing.	£1.5m
6	Regulatory fines	PRA and FCA regulatory fines for operational resilience failures.	£5.0m
7	Regulatory costs	S166 into how breach occurred and validity of actions taken to remediate weaknesses and avoid future occurrences.	£1.0m
8	Business interruption	Lapses on in-force policies, reducing own funds through loss of net present value of future profits.	£120.0m
		Total	£179.5m



Cyber extortion scenario - mitigation

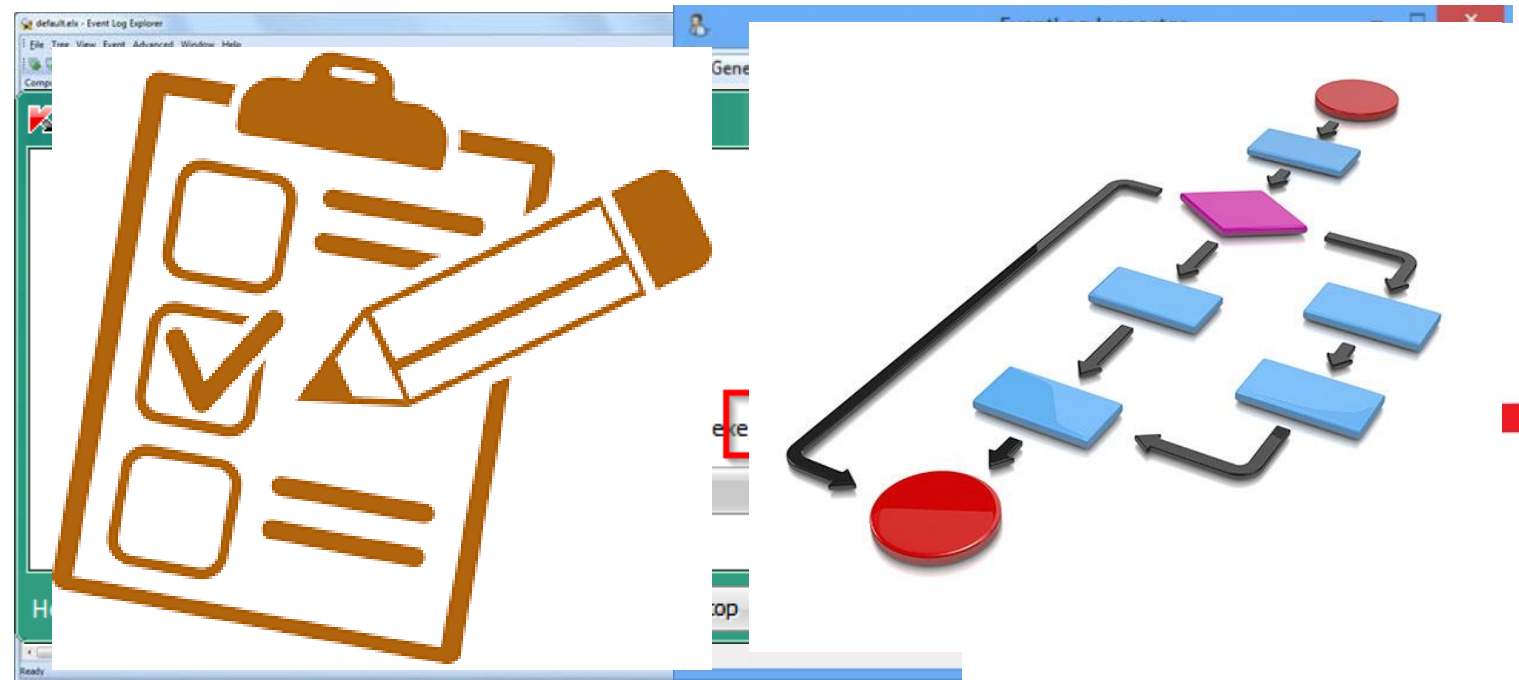


Cyber extortion scenario - mitigation

Detect
(NIST Framework)



2. Detecting and Responding to Events & Monitoring



Institute
and Faculty
of Actuaries

Summary of Results

Scenario:	Employee leaks data at a General Insurer	Cyber extortion at a Life Insurer	Motor insurer telematics device hack
Threat Vector	Insider attack, social engineering	External attack, social engineering	External attack, software vulnerabilities
Security	Protect & respond	Detect, respond & recovery	Identify, protect & detect
Main Cost Components	Compensation, regulatory fines	Business interruption, reputational damage	Remediation (device replacement)
1 in 200 Loss (\$m)	£211m	£180m	£70m



Controls (NIST) Assessment

Summary of the key controls for each scenario that impact the severity and/or the frequency of the event. Key Risk Management and Operational assessment for the scenarios would therefore focus on improving or mitigating these key control areas.

(1) Employee leaks data at a General Insurer	(2) Cyber extortion at a Life Insurer	(3) Motor insurer telematics device hack
<ul style="list-style-type: none"> • Protection e.g. Access Controls, Data Security and Information Protection Processes • Respond e.g. Response Planning, Communication and Improvements 	<ul style="list-style-type: none"> • Detect e.g. Security Continuous Monitoring and Detection Processes • Respond e.g. Analysis, Mitigation and Improvements • Recover e.g. Recovery planning, lessons learned 	<ul style="list-style-type: none"> • Identify e.g. Asset Management & Inventory • Protect e.g. Access Controls, Data Security, Remote Management and Information Protection Processes • Detect e.g. Anomalies and Events



Could Cyber sit under a rule of thumb?

- Different groups
 - Personnel changes
 - Developing cyber environment
- Varying scenarios
- Types and sizes of insurer
 - Differing motives
 - Differing attack perimeters
 - Take Cyber maturity into account
- Estimating a 1 in 200



This is really important!

- Firms need to take Cybersecurity seriously
 - We currently estimate each of these scenarios would be a significant cost to a business (largely driven by required speed of response, fines & regulatory response)
- The NIST framework is a useful place to start when assessing your key Cyber Operational risks
- Figures produced are highly subjective
 - Key uncertainties exists on the likelihood of each scenario and is bespoke depending on each firm.
 - Knowledge/experience varies so widely from person to person
- Communication rationale for scenario selection and cost calculation is important for transparency and development, given speed of development of subject matter



Questions

Comments

The views expressed in this presentation are those of invited contributors and not necessarily those of the IFoA. The IFoA do not endorse any of the views stated, nor any claims or representations made in this [publication/presentation] and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this presentation.

The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this presentation be reproduced without the written permission of the IFoA.



Institute
and Faculty
of Actuaries



Society of Actuaries in Ireland

Consumer Protection Risk

Brian Binchy



SAI Risk Management Perspectives Conference

Conduct & Culture

12 October 2018



Agenda

- 1 What is conduct risk?
- 2 How are firms managing conduct risk?
- 3 Case studies & survey
- 4 What is the role of culture in managing risk?
- 5 What has been the approach undertaken by the Central Bank?
- 6 What is the message for the broader financial services sector?
- 7 What are the typical challenges that firms face?



What is conduct risk?



Conduct risk

In theory

“The risk that firms behaviour will result in poor outcomes for consumers”

International Association of Insurance Supervisors	<p>Conduct of business risk can be described as the risk to customer, insurers, the insurance sector or the insurance market that arises from insurers and/or intermediaries conducting their business in a way that does not ensure fair treatment of customers.</p> <p>Source: International Association of Insurance Supervisors, Issues Paper on Conduct of Business Risk and its Management, 17 June 2015</p>
European Banking Authority	<p>Conduct risk means the current or prospective risk of losses to an institution arising from inappropriate supply of financial services including cases of wilful or negligent misconduct.</p> <p>Source: EBA SREP Guidelines, 19 December 2014</p>
Santander	<p>Conduct Risk is the risk that the business and operational decisions Santander UK takes and the behaviours displayed lead to poor outcomes for our customers.</p> <p>Source: Santander UK Plc 2013 Half Yearly Financial Report</p>
Central Bank of Ireland	<p>Conduct risk is ‘the risk the firm poses to its customers from its direct interaction with them.’</p> <p>Source: PRISM explained, November 2011</p>



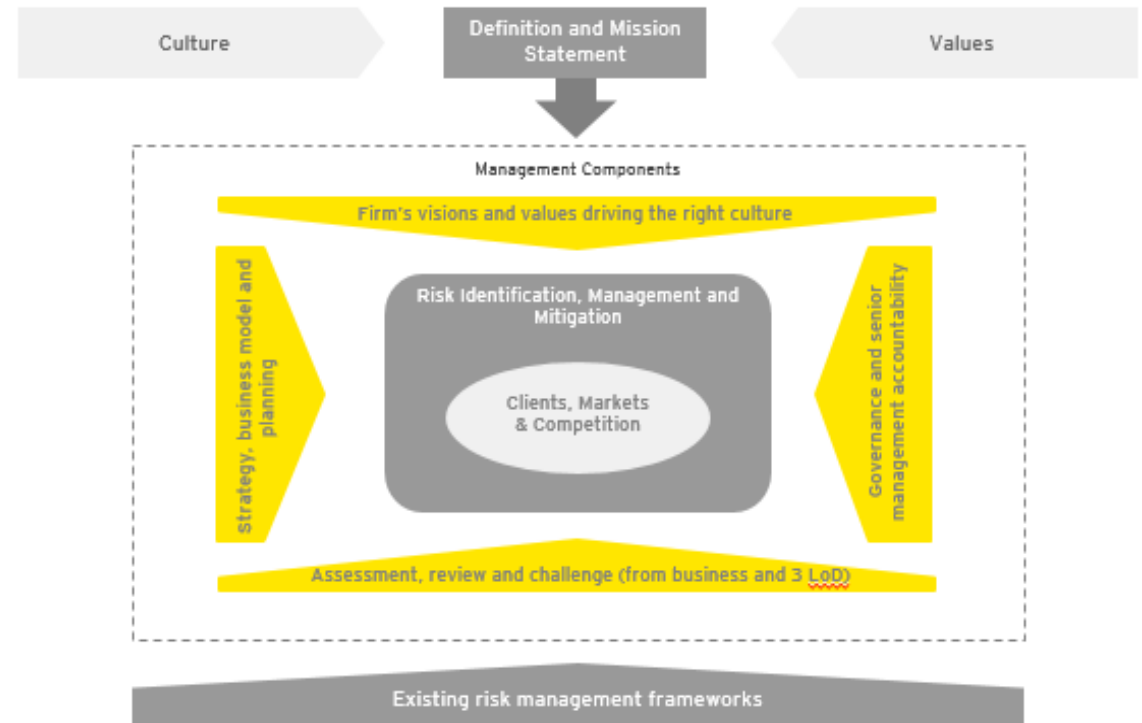
How are firms managing conduct risk?

Conduct risk frameworks

Irish firms have developed components of the framework and must embed the framework to ensure that they can demonstrate effective identification, management and mitigation of conduct risks

Is there clear ownership of conduct risk across the organisation?

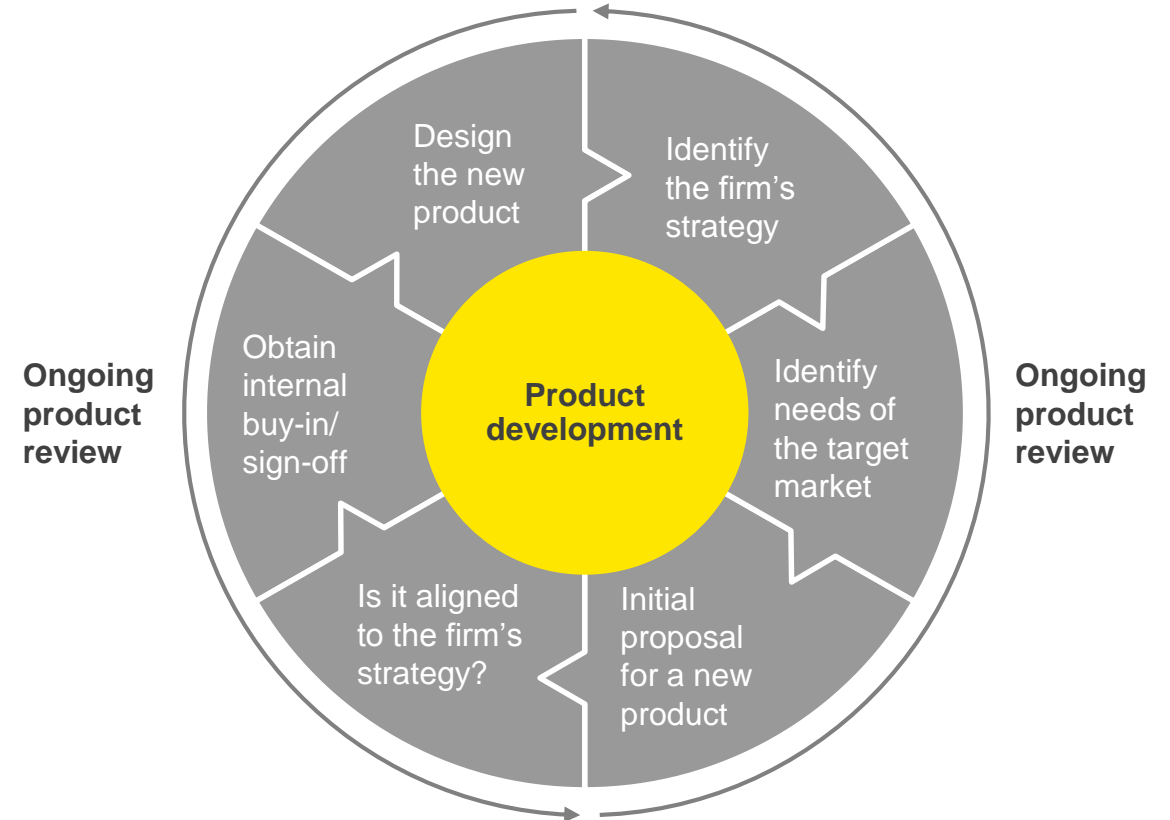
- ▶ Conduct Risk definitions and corresponding risk appetite
- ▶ Reward structures and incentivisation
- ▶ Governance framework and robustness of oversight
- ▶ Lessons learnt
- ▶ Roles and responsibilities
- ▶ Metrics to ensure explicit focus
- ▶ Assessment of control environment



Product governance

Ensuring products behave as planned

- ▶ Firms must have in place effective arrangements to identify issues before they materialise
- ▶ The business has accountability for products from end to end
- ▶ The customer is at the heart of product design and controls must be in place to ensure that the product behaves as planned
- ▶ While new product approval processes and governance have been implemented across firms, product monitoring continues to be enhanced through better MI and more robust periodic review of products on a regular basis



Case studies & Survey



Focus on conduct and culture



"Ten years ago, had you asked me about culture and values I would have rolled my eyes and recited a line from Dilbert. But when I started as CEO I began to appreciate just how important they were. Culture and values provide the foundation upon which everything else is built. They are arguably our most important competitive advantage, and something that has grown to define us."

Jeff Weiner, LinkedIn CEO

Over the past five years, banks have paid out more than US\$300 billion in fines, settlements and restitution as a consequence of malfeasance, malpractice and misconduct.

CCP Research Foundation, Conduct Costs Project Report, August 2017

Conduct and Culture are a recurring theme in both local and global regulatory requirements

Financial Stability Board – Stocktake of Efforts to Strengthen Governance

“In many instances of misconduct, there is evidence that the norms and expectations that most strongly influence behaviour within financial institutions can be very different from the institutions’ stated values and policies. Practice does not always follow principle. Word and deed can diverge. The **culture** of an institution can defeat its formal governance. Indeed, over time the **culture** of a firm can be a major influence on its governance framework”

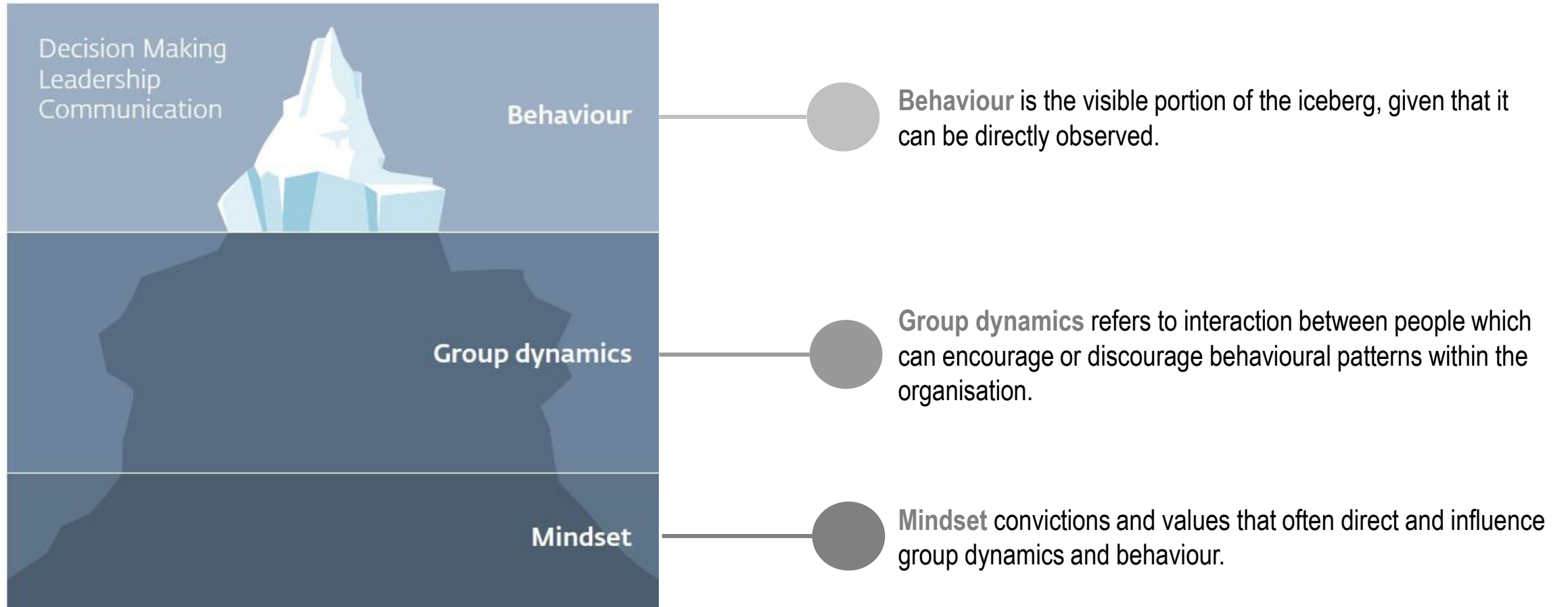
EBA – Guidelines on Internal Governance

“A sound and consistent **risk culture** should be a key element of institutions’ effective risk management and should enable institutions to make sound and informed decisions”

Central Bank of Ireland - CP86, Fund Management Guidance

“Good governance requires clarity as to the allocation of responsibilities, document policies and procedures, structures which foster constructive challenge, and the effective provision of appropriate information to boards. The adoption by a board of the general approach identified [here] will not in itself achieve the objective of good governance. The environment and **culture** in which such an approach operates are also key”

The CBI approach to culture inspections has leveraged the model adopted by the Dutch Central Bank ...



The CBI reported its Report on Behaviour & Culture in Banks in July 2018

Key industry findings

- ▶ A **consumer-focussed culture** has not yet been fully embedded and demonstrated
- ▶ Executives continue to operate in “**fire-fighting**” mode remnant of a crisis era
- ▶ Executives occasionally revert to **directive leadership** styles
- ▶ Institutions are **over-optimistic**
- ▶ There is a **lack of empowerment and decision making** below executives
- ▶ The focus on D&I is relatively recent and the maturity/ambition of approach varies significantly

The findings and actions were included in the CBI's report 'Behaviour and Culture of the Irish Retail Banks' issued on 24 July 2018. Lenders must submit an action plan to the CBI outlining how they will address the CBI's findings.

The CBI is delivering a consistent message on conduct and culture across all sectors of financial services

“Significant cultural issues and challenges in some of the retail banks still exist. Customer interests have not been sufficiently protected or prioritised. This is unacceptable ... ”

Paschal Donohoe, Minister for Finance

“Amid concern that such misconduct can threaten to undermine the safety of financial institutions, there is an emerging trend towards more intensive regulatory focus on governance, conduct and culture issues”

Derville Rowland, Director General Financial Conduct, CBI

“We still encounter the kind of problems which contributed to the financial crisis, such as groupthink, insufficient challenge, poorly assessed risk, and problems with culture – all symptoms of a lack of diversity at the Board and senior management level in many Insurance firms”

Sylvia Cronin, Director of Insurance Supervision, CBI

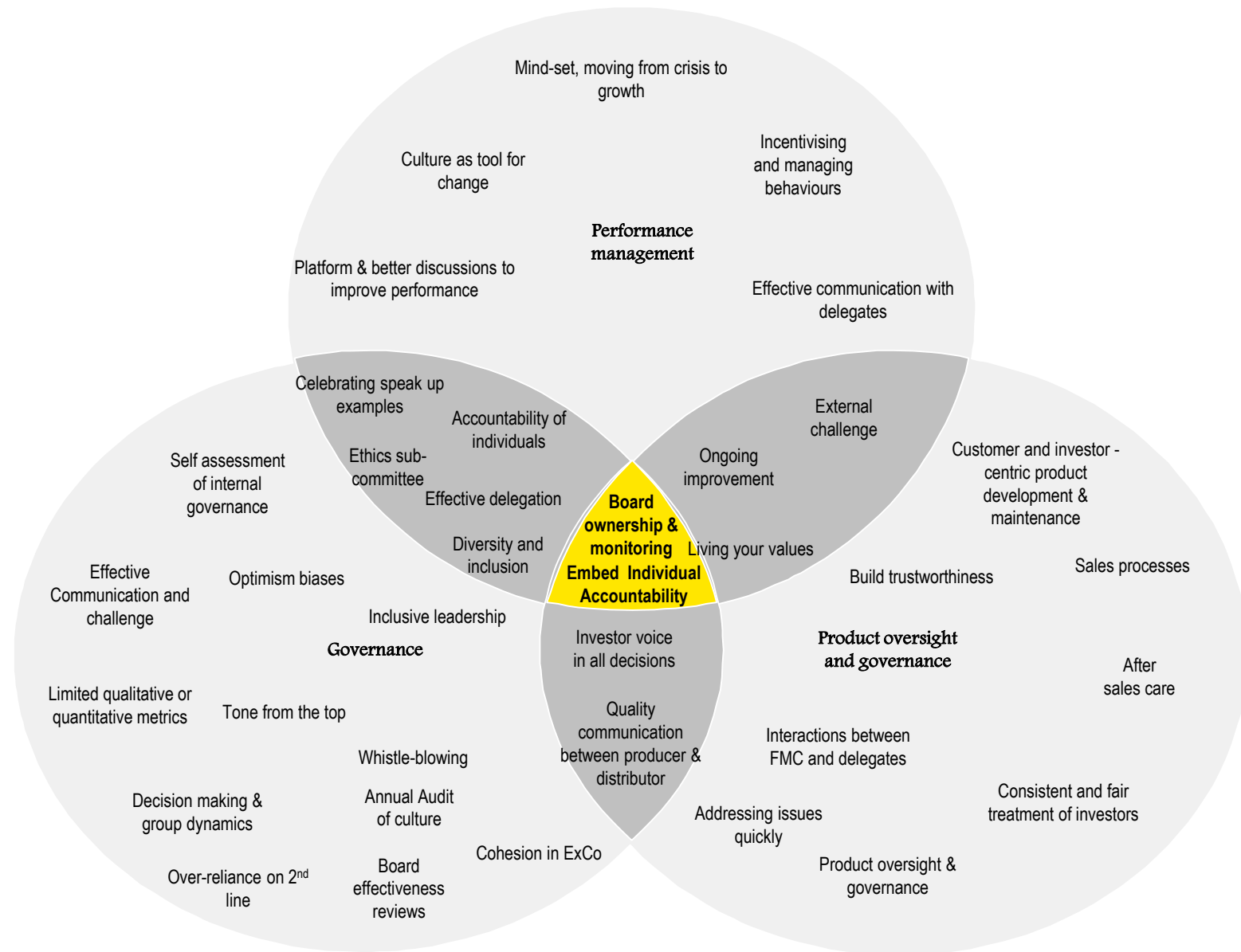
“ ... [T]he culture within an institution ‘drives the values and beliefs which govern how individuals treat others, perform their tasks, take decisions, assess risk, and do the right thing to ensure they operate in a safe and sound manner’. In this regard, board members play an important role in shaping the culture and embedding one that is orientated towards staff doing the right thing even when nobody is watching”

Michael Hodson, Director of Asset Management Supervision, CBI

Each firm should consider what it needs to get right to address the Supervisor's expectations

Call to Action

It is anticipated that more frequent and focussed supervision will be aimed at customer protection and product governance. Firms should be taking on board the increased expectations of Regulators and making the necessary changes



Expect targeted supervision and introduction of an accountability regime

The CBI has flagged what to expect

- ▶ Introduction of an Individual Accountability Framework to include:
 - ▶ Conduct standards
 - ▶ A senior executive accountability regime
 - ▶ Enhancements to the current fitness & probity regime
 - ▶ A unified enforcement process
- ▶ **More frequent and targeted supervision** of high impact firms, emphasising consumer protection and product governance measures
- ▶ Increased **focus on Diversity and Inclusiveness**, placing explicit expectations on institutions regarding D&I policy, governance and plans

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

© 2018 Ernst & Young. Published in Ireland. All Rights Reserved.

749065.pptx. Produced by BSC (Ireland). 9/18. ED none.

The Irish firm Ernst & Young is a member practice of Ernst & Young Global Limited. It is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business in the Republic of Ireland.

Ernst & Young, Harcourt Centre, Harcourt Street, Dublin 2, Ireland.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com



Society of Actuaries in Ireland

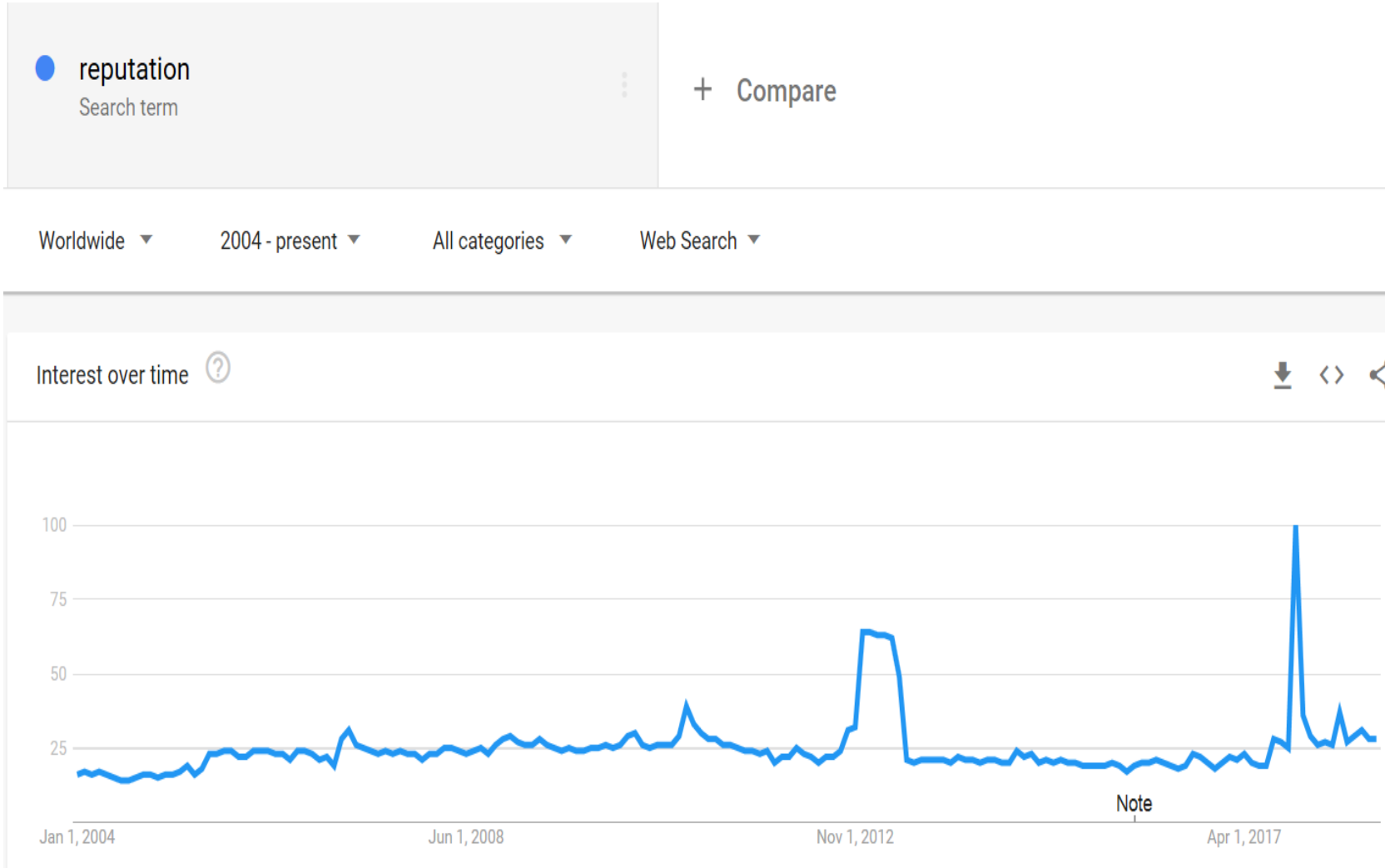
Closing Remarks

Maurice Whyms



Google Trends: “reputation”

(WORLDWIDE)





Google Trends: "reputation"

(WORLDWIDE)

