



Society of Actuaries in Ireland

---

# **Risk Management Perspectives Conference**

---

25<sup>th</sup> October 2017

---



Society of Actuaries in Ireland

---

# **ERM Research Database Risk Survey**

---

25.10.2017

---



# Presentation Format

---

- Over 800 papers on Enterprise Risk Management
  - Users can suggest papers to be added to the database
- The database has been split into several categories
  - General Categories (i.e. common ERM topics)
  - Specific Risk Categories (e.g. credit risk, operational risk)
- The database can be filtered by several headings including;
  - Author
  - Publication Date
  - Publication Type (i.e. Papers or articles)
  - Academic/Commercial Papers



## ERM Resource Database

The ERM Research Database is a collection of articles, papers and books related to Enterprise Risk Management. If you would like to have a resource added to the database or have any feedback in relation to the ERM Resource Database please let us know by using the "Contact us" button below. Some papers require members to log-in due to licensing restrictions.

Users can search the database by general category, specific risk category or by using the keyword search feature. Alternatively you can select all documents to browse the entire database. The database can also be filtered and sorted by using any of the headings shown below.

Please feel free to suggest a new paper or to give feedback on the ERM database.

CONTACT US

Search for results by:

General Category

Specific Risk

Keyword Search

Resource ID

Reset

Title	Published	Author	Publication Type	Resource Type
A Guide to Cyber Risk	2015	Allianz	Article	Commercial
The Road to Improving Risk Culture	2015	Peter Hughes, Allan Grody	Article	Commercial
Heavy Models, Light models and Proxy Models	2014	Institute and Faculty of Actuaries The Proxy Model Working Party: Christopher Hursey*, Matthew Cocke, Cassandra Hannibal, Parit Jakhria, Iain MacIntyre and Matthew Modisett	Paper	Academic
Capital management in a Solvency II world	2014	Milliman: Sinead Clarke, Scott Mitchell, Eamonn O'Keefe	Paper	Commercial

## Trending Articles

### Trending Articles

1. [Capital management in a Solvency II world](#)
2. [Heavy Models, Light models and Proxy Models](#)
3. [The Road to Improving Risk Culture](#)
4. [A Guide to Cyber Risk](#)

### Press & Publications

Annual Review

Briefing Statements

Demography Studies

☐ [ERM Resource Database](#)

☐ [ERM Blog](#)

Newsletters

Papers

Press Releases

Research Projects

Speeches

Strategy Plan

Submissions

User login



# Behavioural Economics and Its Implications for Enterprise Risk Management

Submitted by TheSecretariat on 20 May, 2015 - 13:34

Tagged: [Agency Risk](#) [Behavioural economics](#) [Behavioural Risk](#) [Risk Management Tools and Techniques](#)

The underlying premise of this paper is that enterprise risk management (ERM), as it continues to evolve as both a process and a collection of risk management techniques, can benefit from several different (but ultimately somewhat related) "megatrends." The core of this paper concentrates on the impact on ERM of one of those megatrends: the emergence of a behavioural economics perspective, which is beginning to have a large impact on our understanding of the economy and on certain economic and business processes.

The evolution and context of behavioural economics are described, and potential implications for the practice of ERM are discussed. The paper culminates with a variety of specific suggestions for ERM practice in response to findings from behavioural economics research, specifically a number of human cognitive dissonances which are inconsistent with traditional economic theory.

Source: Society of Actuaries (US)

Length of Resource: 18 pages

Resource File:

 [Click here to download Resource](#)

Author: Rick Gorvett, FCAS, ASA, CERA, MAAA, ARM, FRM, PhD

Date Published: 1 Jan 2012

Publication Type: Paper

Resource Type: Academic

Introduction  
or Summary

Further  
Information



# Survey - learning, development and guidance

---

- Key strategic priority of the ERM Committee is to facilitate and promote learning and development for actuaries in the area of ERM
- Survey conducted during March 2017
- Facilitated gaining an understanding of the needs of members and to tailor future learning and development to meet those needs
- Overview
  - 19 questions, 73 responses, approx. 33% response rate.
- Output is being used to drive the ERM committee learning agenda in the following areas:
  - forms of learning and development, e.g. evening meetings,
  - Hot topics; and
  - Insight relating to the ERM resource database.

# 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

---

# **Brexit – Views from the former Chair of the Seanad Brexit Committee**

---

Senator Neale Richmond

---





Banc Ceannais na hÉireann  
Central Bank of Ireland

Eurosystem

# Operational Risk Assessments Perspectives from the Central Bank of Ireland ('CBI')

*Lisa O'Mahony, Head of Function, On-site Inspections  
Insurance Supervision Division*

25 October 2017

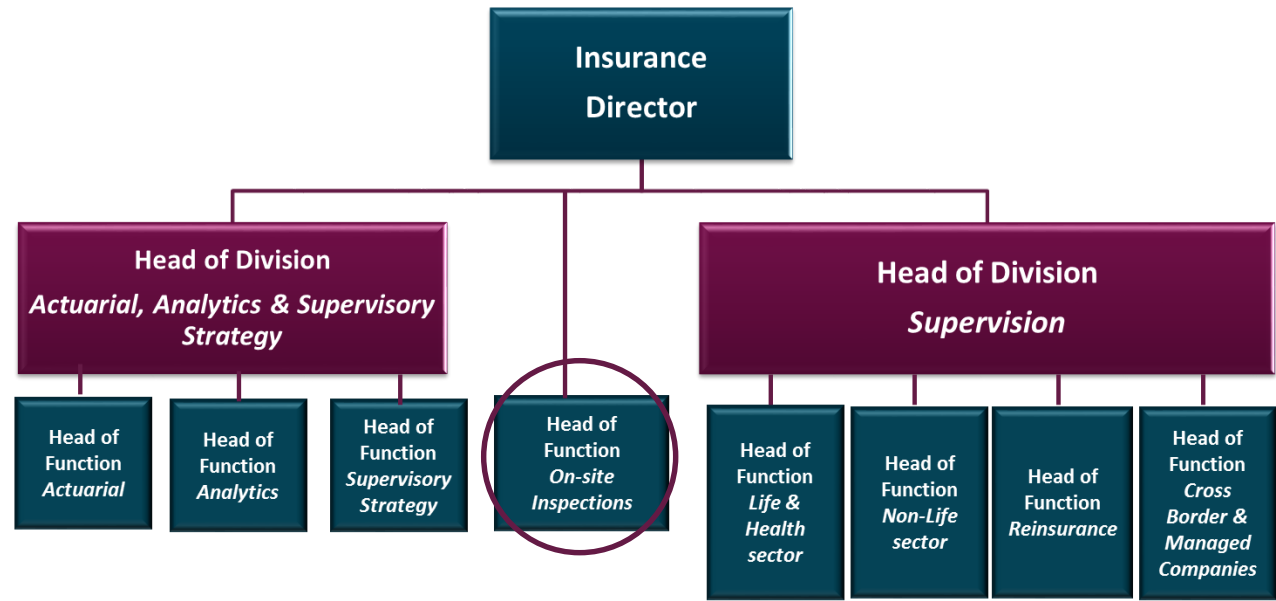


## Introduction



**Lisa O' Mahony**, *Bsc, MAcc, ACA, CTC*

Head of Function - On-site Inspections,  
Insurance Supervision Directorate,  
The Central Bank of Ireland.





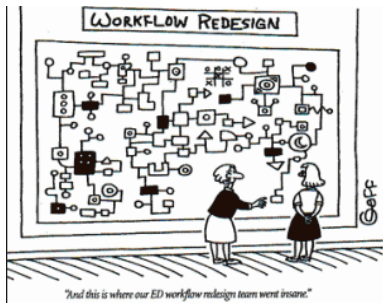
## Agenda

---

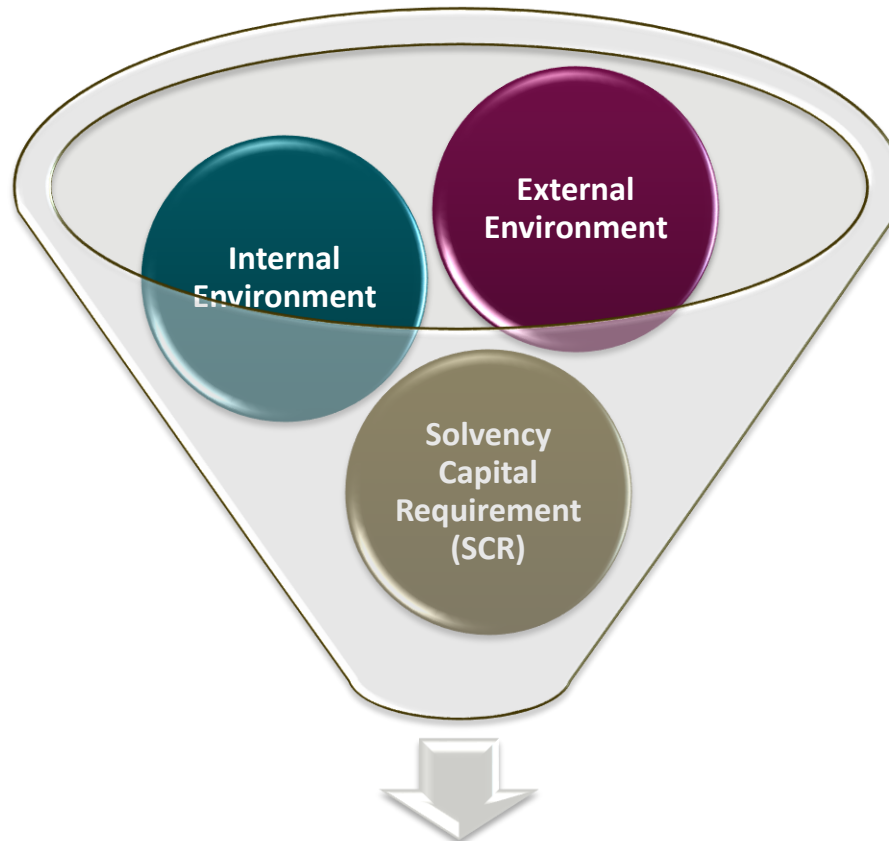




## Why Operational Risk?



Credit: [www.thegramewhite.com](http://www.thegramewhite.com)



**Financial, Reputational &  
Operating Impacts**



Credit: [www.ibtimes.co.uk](http://www.ibtimes.co.uk)

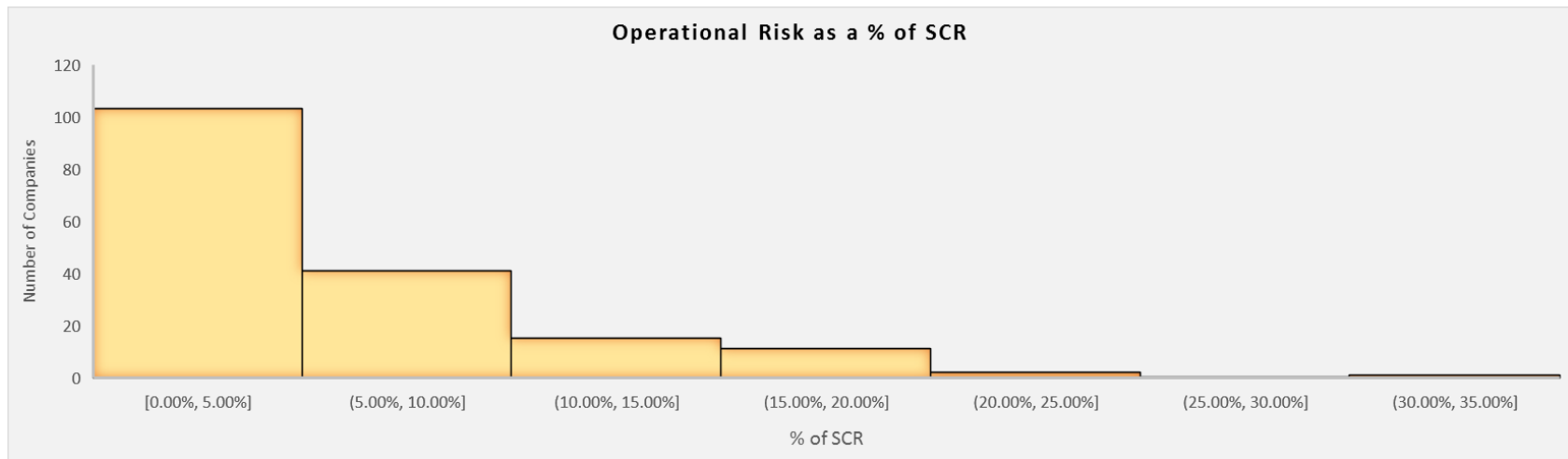


Credit: [www.drykings.com](http://www.drykings.com)





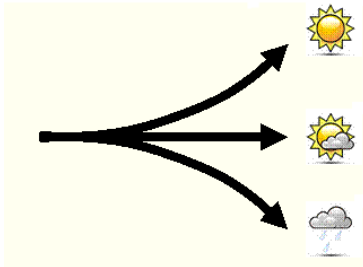
## Operational Risk and the SCR



- This chart shows all companies, supervised by the Central Bank of Ireland across all sectors and all impact categories.
- The majority of companies have stated operational risk as being between 0% and c.7% of the SCR.
- Only a handful of companies have stated operational risk as being 20%+ of the SCR.
- Across all companies, the average is 6.7% of the SCR.



## Risk Identification



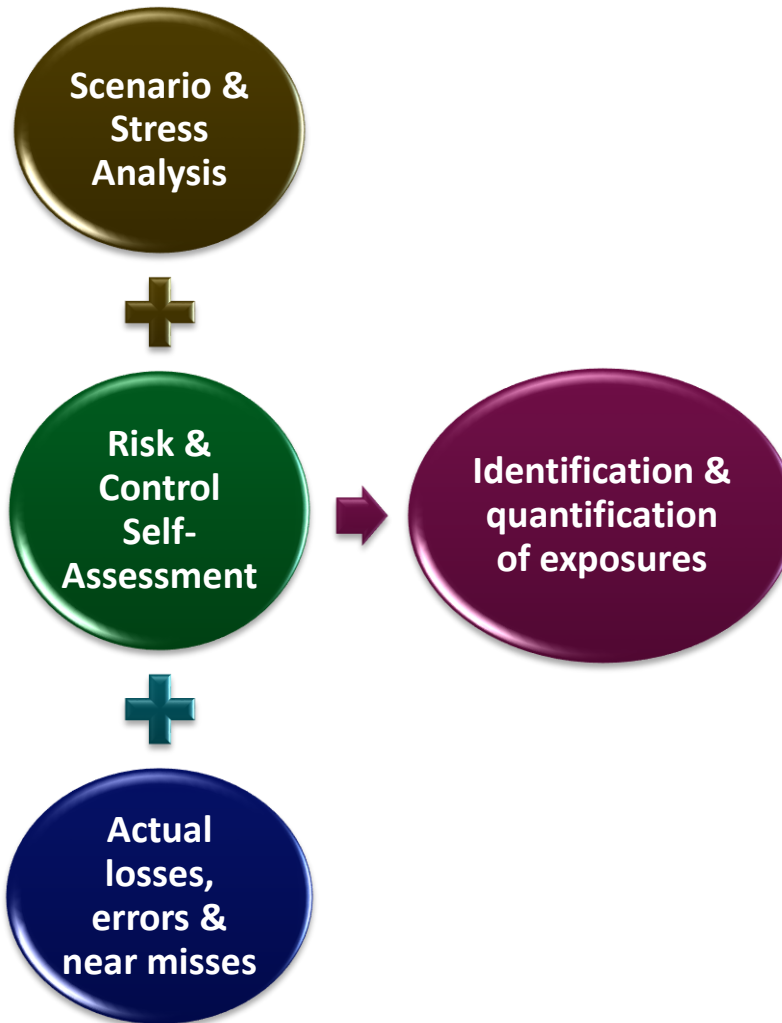
Credit: [www.12manage.com](http://www.12manage.com)



Credit: [www.12manage.com](http://www.12manage.com)

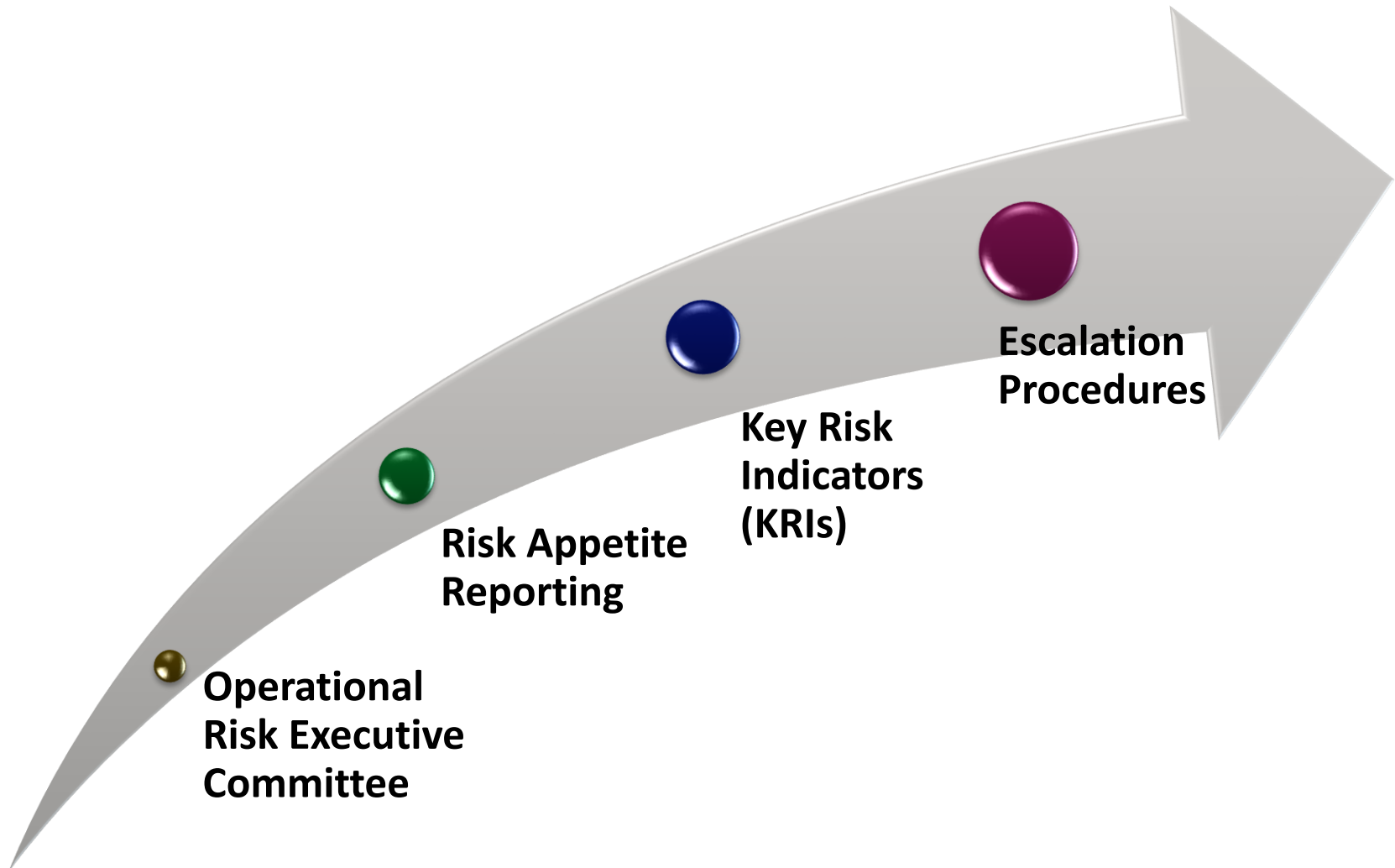


Credit: [www.osholutions.com](http://www.osholutions.com)



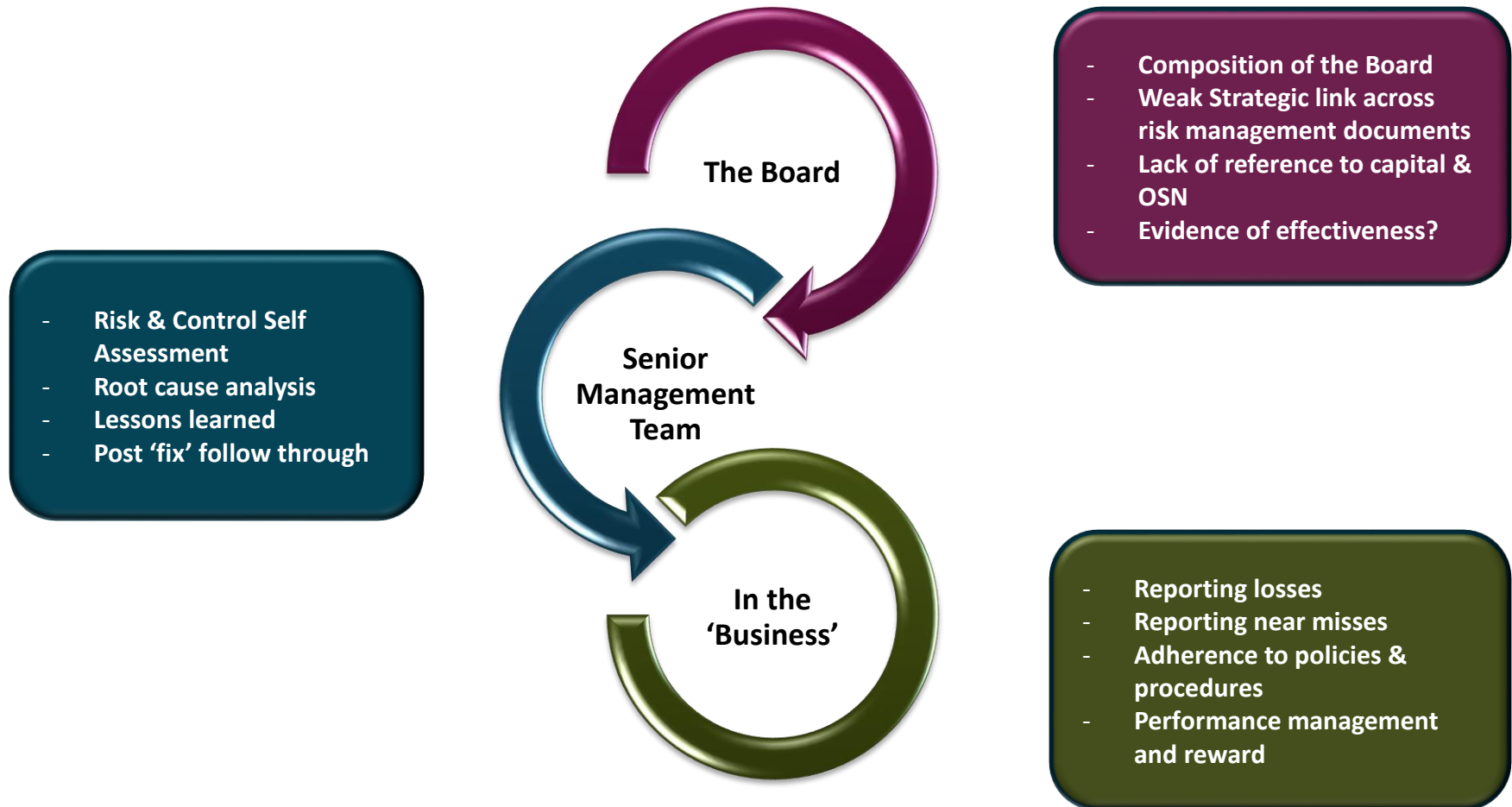


## Risk Monitoring and Reporting





## Risk Culture







## Conclusion



Credit: [www.smartforlife.com](http://www.smartforlife.com)





# Thank You

**Contact information:**

email: [lisa.omahony@centralbank.ie](mailto:lisa.omahony@centralbank.ie)

Tel: 01 224 4839

I am grateful to Lenka Marsikova, Susan Forristal and Fiona Brosnan for their contributions to this speech.



Society of Actuaries in Ireland

---

# **Cyber risk audits – Common themes arising and update on points of focus**

---

Michael Daughton

---



# Definition

---

**“Cyber risk is loss or damage arising out of unauthorised access to, use of, disclosure of, disruption of, modification or destruction to information and information systems”.**



# Starting point

**86%** of CEOs are concerned about the loyalty of their customers

**72%** of CEOs are struggling to keep up with new technologies

of CEOs are concerned about the relevance of their products and services **66%**

**29%** of CEOs list cyber as the issue that has the biggest impact on their company today

of CEOs indicated that information security/cyber is the risk they are most concerned about **20%**

## Are you able to sleep at night

- KPMG International surveyed over 1,200 chief executives from many of the world's largest and most complex companies and discovered what keeps them awake at night.
- C-suite and board members traditionally have viewed cyber security as a tactical problem, not a strategic issue. Over the past decade, there is realization that cyber security can pose an enterprise-wide risk.



# Cyber Security: A Boardroom Priority

**“The complex interconnectedness of financial institutions and markets means that the financial system is only as strong as the weakest link in the chain. This is why the presence of cyber security risks in one firm could potentially give rise to systemic failure. So far we have not had a cyber-event that led to systemic problems but it may be only a matter of time. A seemingly manageable security incident at a single firm could cascade quickly to the broader financial sector.”**

Address by Deputy Governor, Cyril Roux,  
Society of Actuaries in Ireland Risk Management Conference,  
“Cybersecurity and Cyber Risk”, 30 September 2015



# From the frontline

---

## Organisation's are facing a perfect storm of:

- Technology developing in leaps and bounds
- Increased erosion of perimeter from third parties, social media and personal devices
- Increasing number of vulnerabilities
- Rapidly evolving threat landscape with incidents on the rise and with increasing business impact
- Attacks increasingly targeted
- Attackers increasingly using multiple attack routes
- Those who have been breached often may not be aware of compromise
- Companies fighting a moving and evolving target
- Traditional means of crime and extortion being “digitised”
- Risk outpacing organisation's ability to keep up



# Key security trends

## 1 Threats

- Organized crime
- Nation states
- Cyber espionage
- Hactivism
- Insider threats

## 3 Rapid technology change

- Critical national infrastructure
- Smart / metering
- Digital transformation
- Internet of things
- Industry 4.0

## 5 Changing market and client need

- Strategic shift
- Situational awareness
- Intelligence sharing
- Cyber response

## 2 Change in the way business is conducted

- Cloud computing
- Big data
- Social media (Twitter,...)
- Consumerization
- Bring your own device (BYOD)
- Mobile banking

## 4 Regulatory compliance

- Data loss
- Privacy
- Records management





# Cyber imapcts – What is at stake?





# Cyber Security – 2017 KPMG Global Audit Committee Institute Survey

---

**35% of Irish members are satisfied with their level of focus on managing cyber security risk**

**At a global level 25% of members are satisfied despite the issue being identified as a key challenge by committee members.**

**In general, audit committees identify cyber security risk among their top challenges**

**Almost one third of the 800 audit committee members surveyed said that additional expertise related to technology and cyber security would be helpful**

**Audit Committees looking to the Internal Audit function to focus on critical risks to the business, including cyber security risk**



# The five most common Cyber Security mistakes

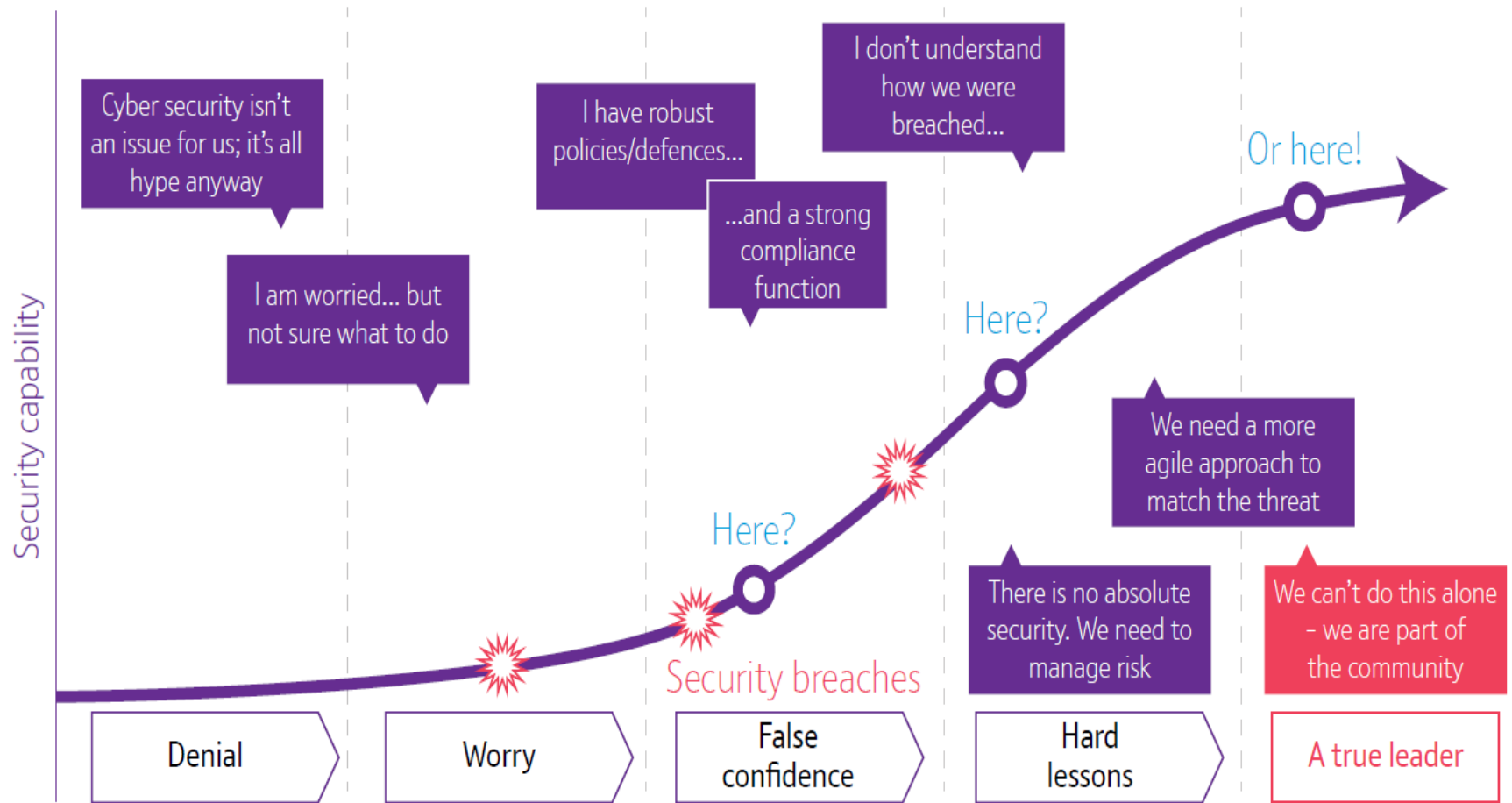
To many, cyber security is a bit of a mystery. This lack of understanding has created many misconceptions among management about how to approach cyber security.

The following five cyber security mistakes are repeated over and over—often with drastic results.

Cyber security mistakes		Reality
1	We have to achieve 100 percent security.	The goal of 100 percent security is neither feasible nor appropriate.
2	When we invest in best-of-class technical tools, we are safe.	Effective cyber security is less dependent on technology than you think.
3	Our weapons have to be better than those of the hackers.	The security policy should primarily be determined by your goals, not those of your attackers.
4	Cyber security compliance is all about effective monitoring.	The ability to learn is just as important as the ability to monitor.
5	We need to recruit the most suitable professionals to defend ourselves from cyber crime.	Cyber security is not a department, but an attitude.



# Cyber Resilience: A journey not a project





# The four golden rules of Cyber Security

---

## **Get the basics right.**

Over 75 percent of attacks exploit failures to put in place basic controls.

## **Look after your crown jewels.**

You have to prioritize where you spend your money to defend yourself, so build a fortress around your most critical assets.

## **Do your homework on your enemies.**

Invest in understanding who might attack you, why and how so that you can anticipate the most likely scenarios and you defend those assets that are most likely to get attacked.

## **Treat cyber risk as an opportunity to look closely at your business.**

Security and resilience can affect nearly every part of an organization. Strategies to protect IT security and business resilience should align with an organization's broader goals — from protecting intellectual property to maximizing productivity to finding new ways to delight customers.



# Cyber Resilience: get the basics right

---

Raise awareness

Start with good  
housekeeping:  
firewalls, anti-virus,  
patching, password  
security and backups

Inventory  
your assets

Make sure everyone  
has a responsibility for  
cyber security

Train your people  
in security

Be ready  
to respond

Focus on investing in  
protecting your most  
sensitive information



# The Six dimensions - KPMG Cyber Maturity Framework

Technology alone is not the answer to Cyber risk issues. The answer lies in an integrated approach, focusing on all elements identified below.

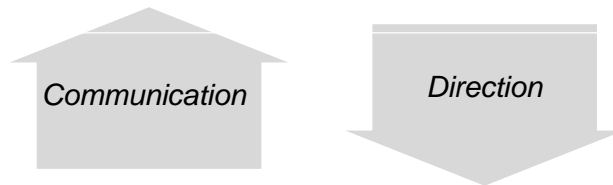




# Leadership and Governance

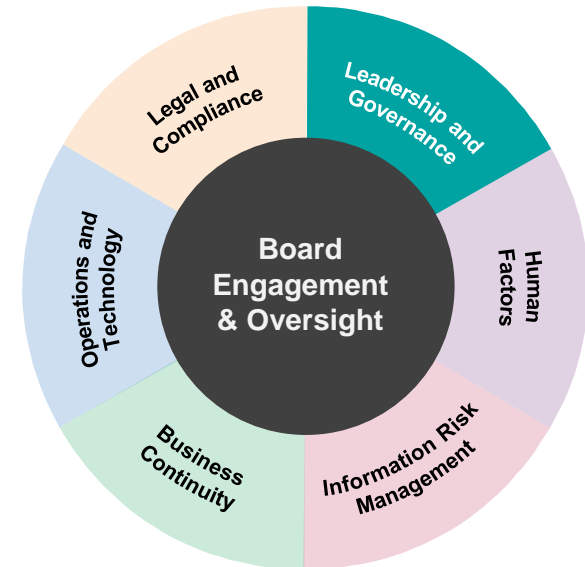
## How should boards engage?

- Understand governance structure and meet executive leadership team
- Review output of capability assessment
- Review and approve strategy and funding requests
- Participate in general board education
- Request periodic updates of program



## What should management do?

- Define program ownership and governance structure
- Identify sensitive data assets
- Inventory third-party supplier relationships
- Perform assessment of current capabilities
- Define a strategy and approach
- Educate the board and executive management



## LEADERSHIP AND GOVERNANCE

Management demonstrating due diligence, ownership, and effective management of risk





# Human Factors

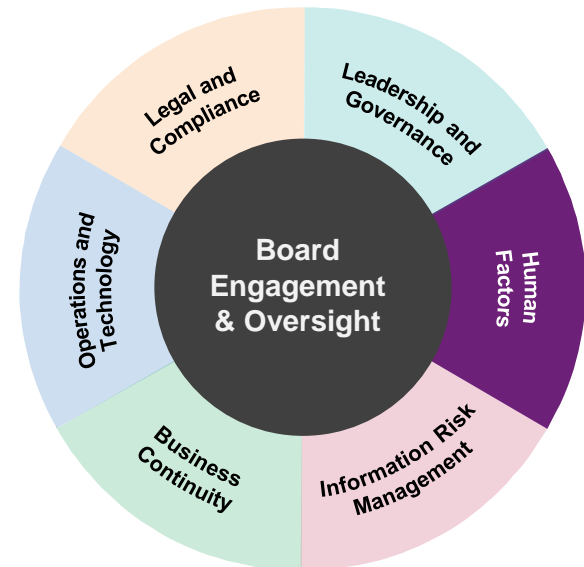
## How should boards engage?

- Set the tone for the culture
- Review patterns/trends of personnel issues
- Understand training & awareness protocols



## What should management do?

- Define culture and expectations
- Implement general training and awareness programs
- Implement personnel security measures
- Define talent management and career architecture
- Develop specific learning paths for key personnel



## HUMAN FACTORS

The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge



# Information Risk Management

## How should boards engage?

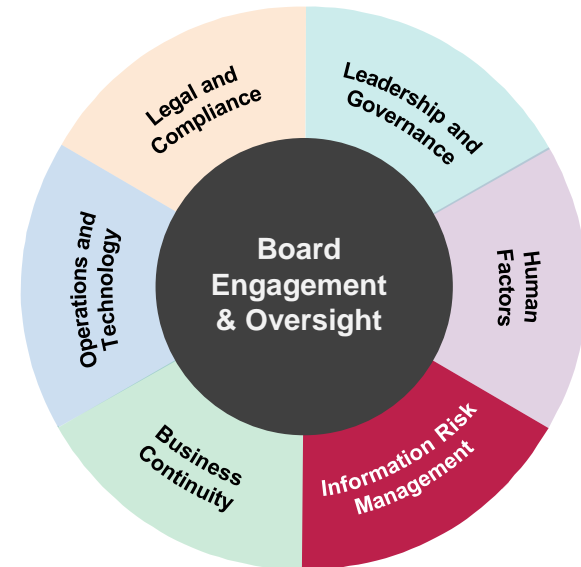
- Understand risk management approach and linkage to enterprise risk
- Review and approve risk tolerance
- Understand third-party supplier program
- Review and question program metrics

Communication

Direction

## What should management do?

- Develop risk management approach and policies
- Identify risk tolerance and communicate
- Link risks to sensitive data assets
- Perform risk assessment and measures
- Perform third-party supplier accreditation
- Report relevant metrics



## CYBER RISK MANAGEMENT

The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners



# Incident, Crisis and Business Continuity Management

## How should boards engage?

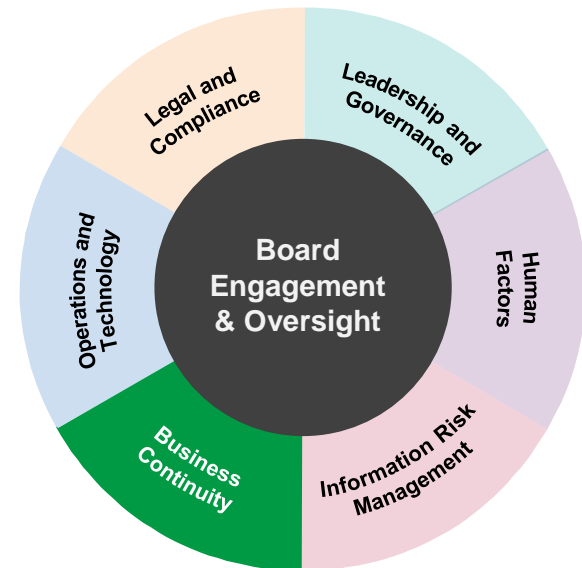
- Understand current response capability
- Review status of overall plan maturity
- Meet with communications personnel
- Participate in table-top exercises

*Communication*

*Direction*

## What should management do?

- Assess current ability to manage cyber events
- Perform analysis of risks and financial requirements
- Develop robust plans
- Assign resources and develop training
- Integrate with corporate communications
- Perform testing of plans



## INCIDENT, CRISIS AND BUSINESS CONTINUITY MANAGEMENT

Preparations for a security event and ability to prevent or minimize the impact through successful crisis and stakeholder management



# Operations and Technology

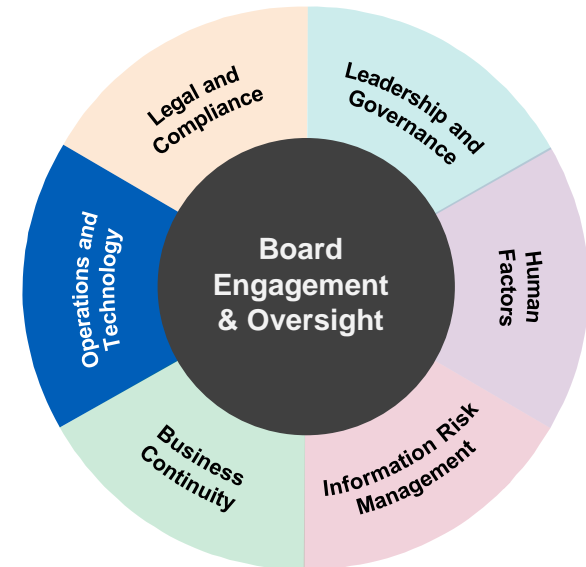
## How should boards engage?

- Understand current maturity of control structure
- Review relevancy of selected control framework
- Review relevant incident trend metrics
- Meet with CISO or equivalent to understand integration of cyber and information technology trends



## What should management do?

- Select and implement a control framework
- Implement logical and physical security controls
- Perform threat and vulnerability management
- Perform security monitoring
- Implement incident response capabilities
- Integrate activities with broader IT service management



## OPERATIONS AND TECHNOLOGY

The level of control measures implemented to address identified risks and minimize the impact of compromise



# Legal and Compliance

## How should boards engage?

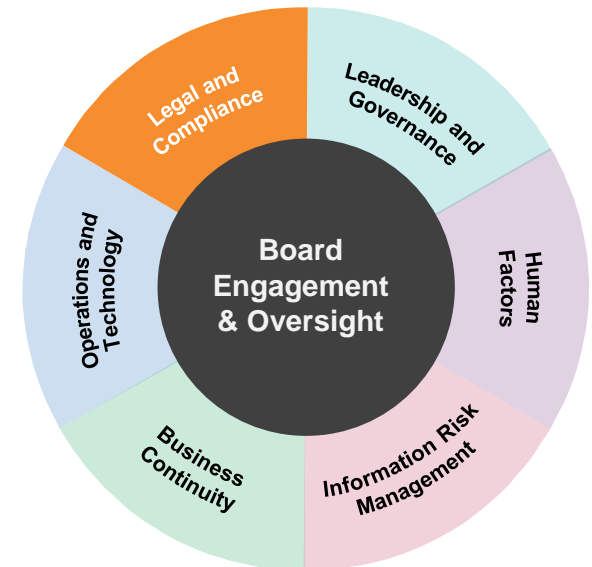
- Understand regulatory landscape impacting the organization
- Clarify audit committee requirements for cyber
- Review litigating inventory trends
- Review and approve cyber insurance funding (if relevant)

*Communication*

*Direction*

## What should management do?

- Catalog all relevant compliance requirements
- Link compliance requirements to control framework
- Formalize the role of the audit committee
- Develop litigation inventory and trending
- Analyze and recommend need for cyber insurance



## LEGAL AND COMPLIANCE

The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge



# **CBI expectations for Managing Cybersecurity Risk**

- Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks
  - Issued by the Central Bank in September 2016
  - 13 expectations for Cybersecurity risk management
- CBI expects Boards and Senior Management of regulated firms to fully recognise their responsibilities in relation to IT and cybersecurity governance and risk management and place these among their top priorities
- While advancements in technology have introduced a number of customer and firm benefits, they also bring significant risks, as firms become increasingly interconnected and more reliant on complex IT systems and outsourcing service providers to conduct their business and deliver services to customers
- Clear communication that the failure of a firm's IT systems can have significant adverse financial, legal, customer and reputational consequences that should not be underestimated
- SSM on-site methodology on Cybersecurity
  - Aligned to NIST Framework for Cybersecurity
  - Identify / Protect / Detect / Respond / Recover



# Cyber Security – An Internal Audit perspective

All Boards, should with the help of Internal Audit, have a view of the organisation's response to the rising cyber threat and the quality of its cyber governance and risk management.

## **Some initial key questions and considerations:**

- Has the organisation recognised the potential threat to business resilience, reputation and even revenues that cyber risk poses?
- Are key controls in place and / or has a recognised framework been implemented?
- Does the organisation understand which of its data assets are most valuable and have they been mapped?
- Does the organisation have effective and updated firewalls and malware protection in place?
- Are existing protections being effectively tested?
- Is the governance around access rights sufficiently robust?
- Is the organisation staying abreast of developing threats and emerging cyber attacks?
- Have cyber risk training and awareness sessions been held across the organisation and are policies reflected in employee behaviour?
- Is the organisation prepared to respond to and recover in the likely event of an attack?



# Some Food for Thought

---

- World economic forum quotes global cost of cybercrime as high as \$3 trillion dollars – more profitable than the drug trade.
- Average number of days from breach to discovery is 289 days
- 70% of breaches are reported externally rather than internally. Some organisations are not likely to get external reports.

**“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again”.**

Robert S. Mueller III, Director Federal Bureau of Investigation





# How to Protect Your Organisation – illustrative for example

---

- Board level **awareness** needs to be raised
- Move from compliance based to **risk based security** strategies
- **Identify and rank** your assets
- Compare **cyber-maturity** to your peers – are you the easy target?
- End to End **encryption** – data at rest, transit, key storage & loss
- Base-lining & outlier **tracking**
- **Privileged user** monitoring & SOD
- Strict password & **authentication** policies – introduce 2 Factor Authentication

- **Security Operation Centres** for monitoring
- Use of external **reputation** monitoring
- **Staff focus** – on-boarding, training, atypical usage
- **Network** segmentation and perimeter monitoring – file transfers
- **Third party** vetting and interfaces
- Acquisition **cyber risk assessments**
- Tighter **mobile device** & BYOD policies
- Cyber **insurance**



# Some Questions for Board and Management (and Internal Audit)

---

- 1 Who is accountable for security within your organisation? How clear is your governance over cyber security and incidents?
- 2 Are you having conversations around cyber risks internally? What are your key risks?
- 3 What is your cyber security strategy – People/Process/Technology and Protect/Detect/Respond?
- 4 Do you know what the latest fines are for data breaches?
- 5 Do you know where your critical data (“crown jewels”) is stored and who has access to it?
- 6 Do you think you are aware of all of your obligations for information assurance?
- 7 Have you rehearsed a cyber event scenario as part of crisis management?
- 8 How do you keep ahead of cyber attackers? How many information risks have been escalated?
- 9 How are you managing the risk that new technologies like cloud, social media, and Big Data bring to ensure that you get the benefits?
- 10 Have you completed an assessment of your Cyber security controls?
- 11 How do you manage the risks in relation to third parties?



# EU GDPR at a Glance

The General Data Protection Regulation or GDPR was adopted on 27 April 2016. It will apply starting on 25 May 2018, after a two-year transition period. It is immediately enforceable as law in all member states of the European Union. The primary objectives of the GDPR are to institute citizens' rights in controlling their personal data and to simplify the regulatory business environment by a unified regulation within the EU.

## Legal changes

- Expansive jurisdiction
- One European legislation
- Processors can be held accountable

## Authority oversight

- European Data Protection Board
- One lead supervisory authority
- Obligated data breach notification
- High fines in case of violations
- Certification schemes (seals)



## Citizens right

- Stricter conditions for consent
- Right to rectification
- Right to erasure, right to be forgotten
- Right to restriction of processing
- Right to data portability
- Right to object and automated individual decision-making

## Organisational measures

- Data Protection officer (DPO)
- Accountability
- Data Protection impact assessment (DPIA)
- Inventory of all personal data
- Data protection by design and by default



# Questions and Answers

Society of Actuaries in Ireland  
Risk Management Perspectives Conference  
Geopolitical Risk and Macroeconomic Update

Jim Power

October 25<sup>th</sup> 2017

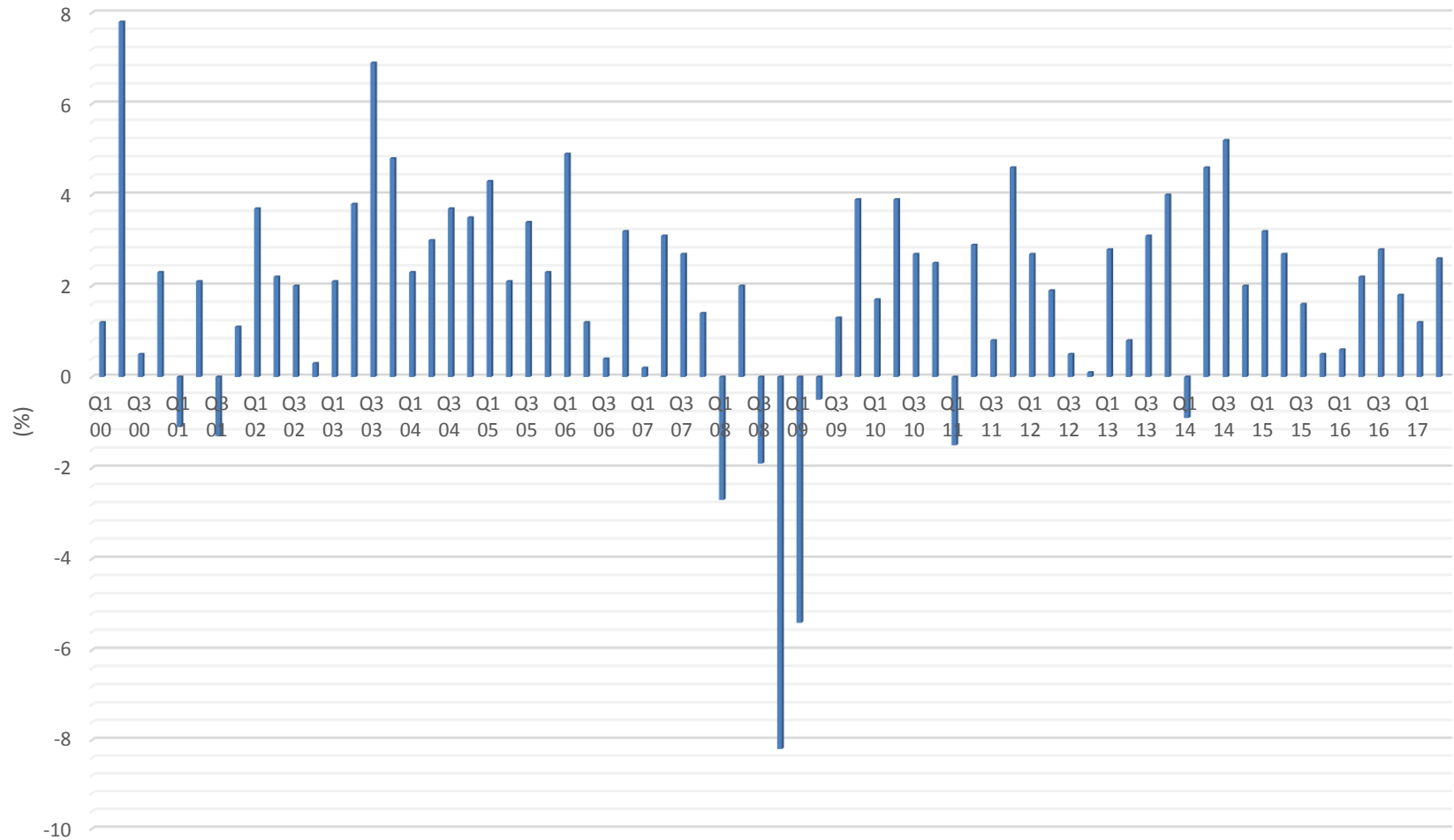
# To Be Discussed

- Global Economic Backdrop
- Global Economic Risks
- Global Geopolitical Risks
- Update on Irish Economy

## **GLOBAL ECONOMIC BACKDROP**

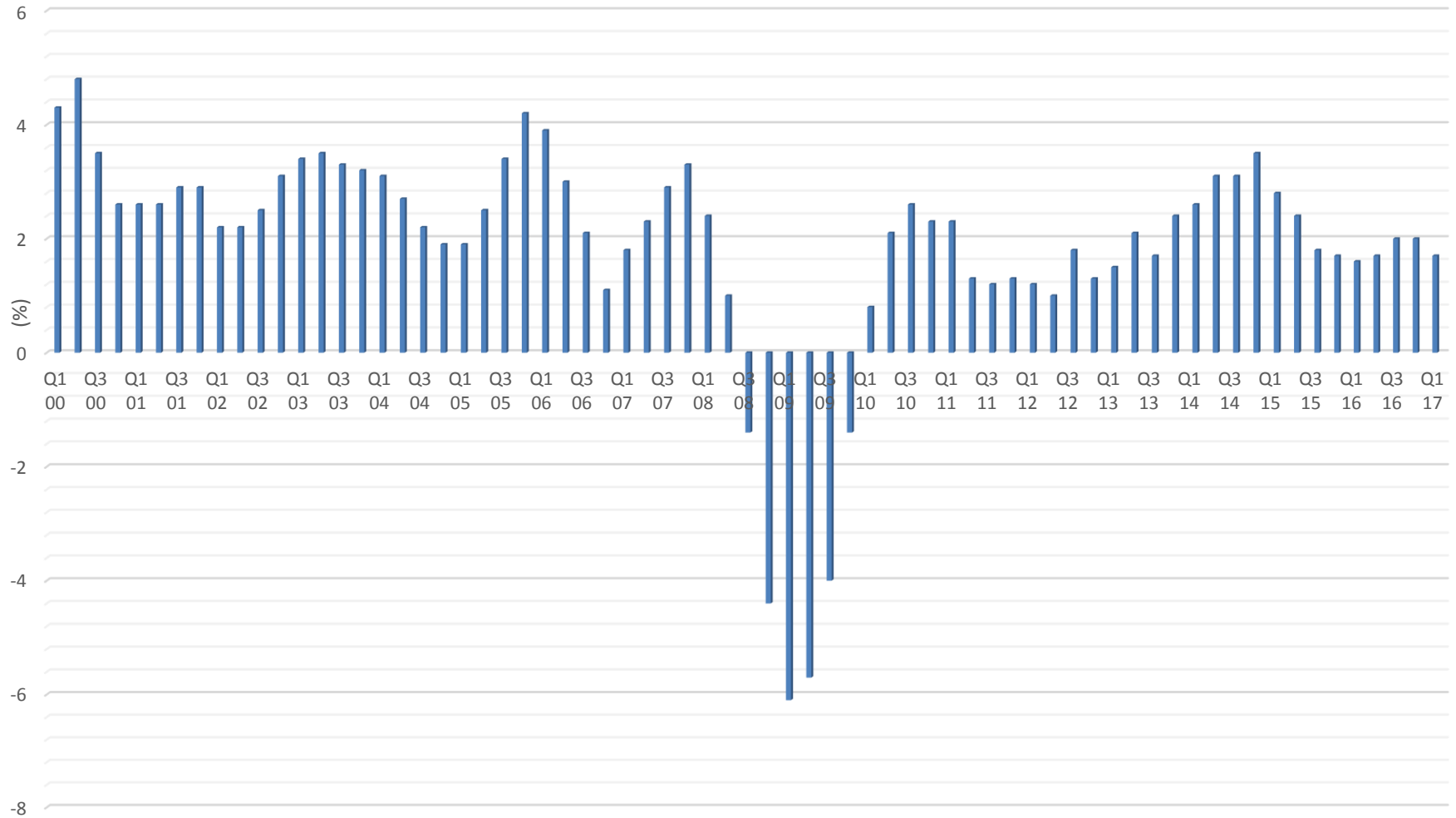
- 2017 a better year for global economy
- US growth reasonable; inflation moderate
- UK held up well post-Brexit > sterling weakness helped exports, but consumer & business investment coming under some strain
- Euro Zone growth recovery becoming more broad-based
- Chinese growth has stabilised
- Global growth story reasonably compelling

# US GDP (YoY)

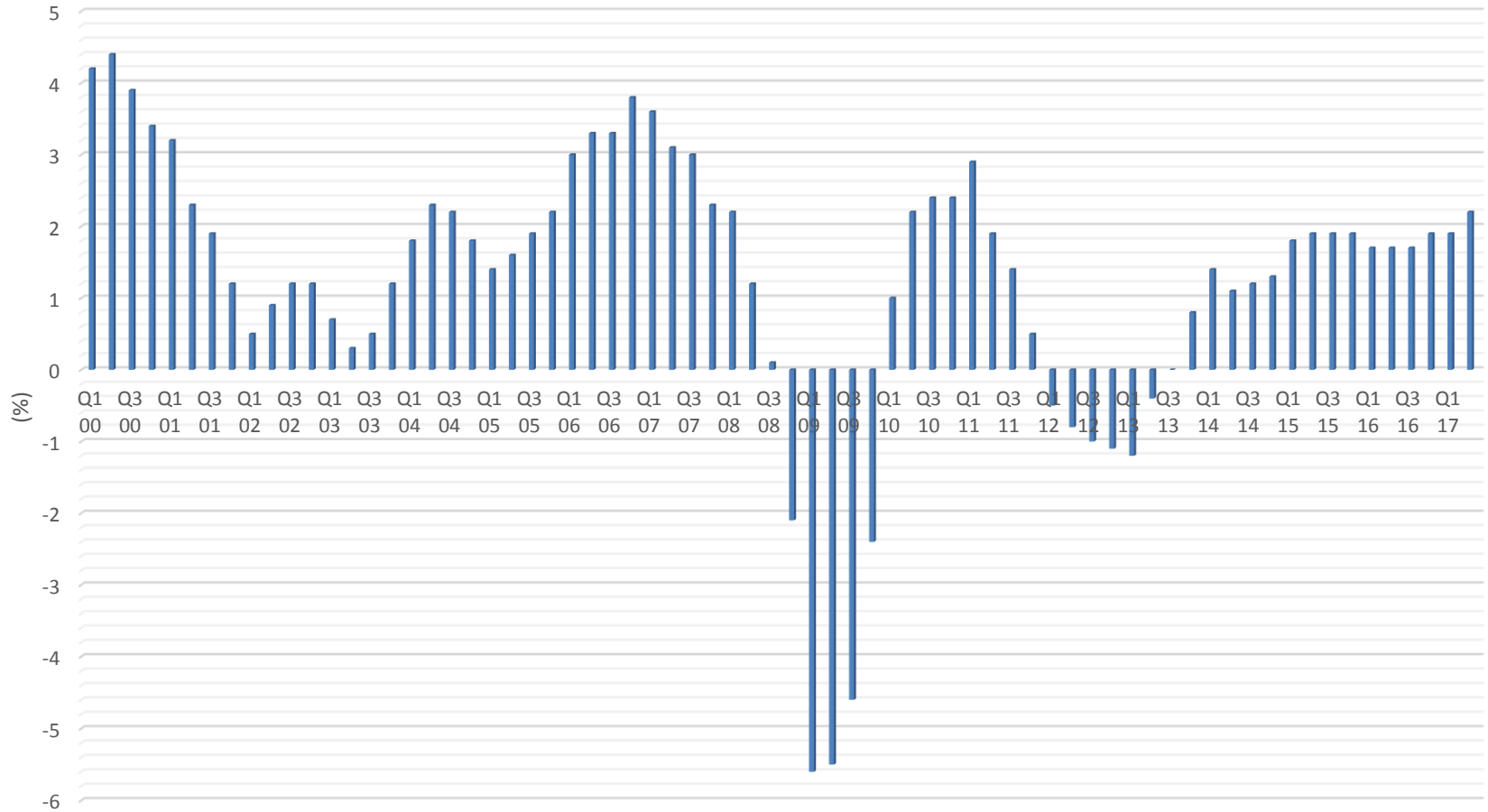




# UK GDP (YoY)



# Euro Zone GDP (YoY)



# Strange Environment

- Inflation muted in most parts of developed world
- US Fed Funds up from 0% to 1.25% since Dec 15
- ECB Rates Refinancing Rate 0%, Bank Deposit Rate -0.4% > no pressure for the moment
- UK Base Rate 0.25% > some pressure
- Bond Yields close to historically low levels
- Equity markets have come a long way since Q1 2009

# Global Growth Forecast

(IMF OCT 17)	2016	2017f	2018f
World Output	+3.2%	+3.6%	+3.7%
Advanced	+1.7%	+2.2%	+2.0%
US	+1.5%	+2.2%	+2.3%
Euro Zone	+1.8%	+2.1%	+1.9%
-Germany	+1.9%	+2.0%	+1.8%
-France	+1.2%	+1.6%	+1.8%
UK	+1.8%	+1.7%	+1.5%
Japan	+1.0%	+1.5%	+0.7%
Emerging	+4.3%	+4.6%	+4.9%
China	+6.7%	+6.8%	+6.5%
India	+7.1%	+6.7%	+7.4%

# Global Economic Risks

- Brexit
- Trump & Protectionism
- Reversal of QE
- Official interest rate cycle
- China & its imbalances
- Rollback of financial regulation
- Equity markets have come a long way
- Extreme weather related events

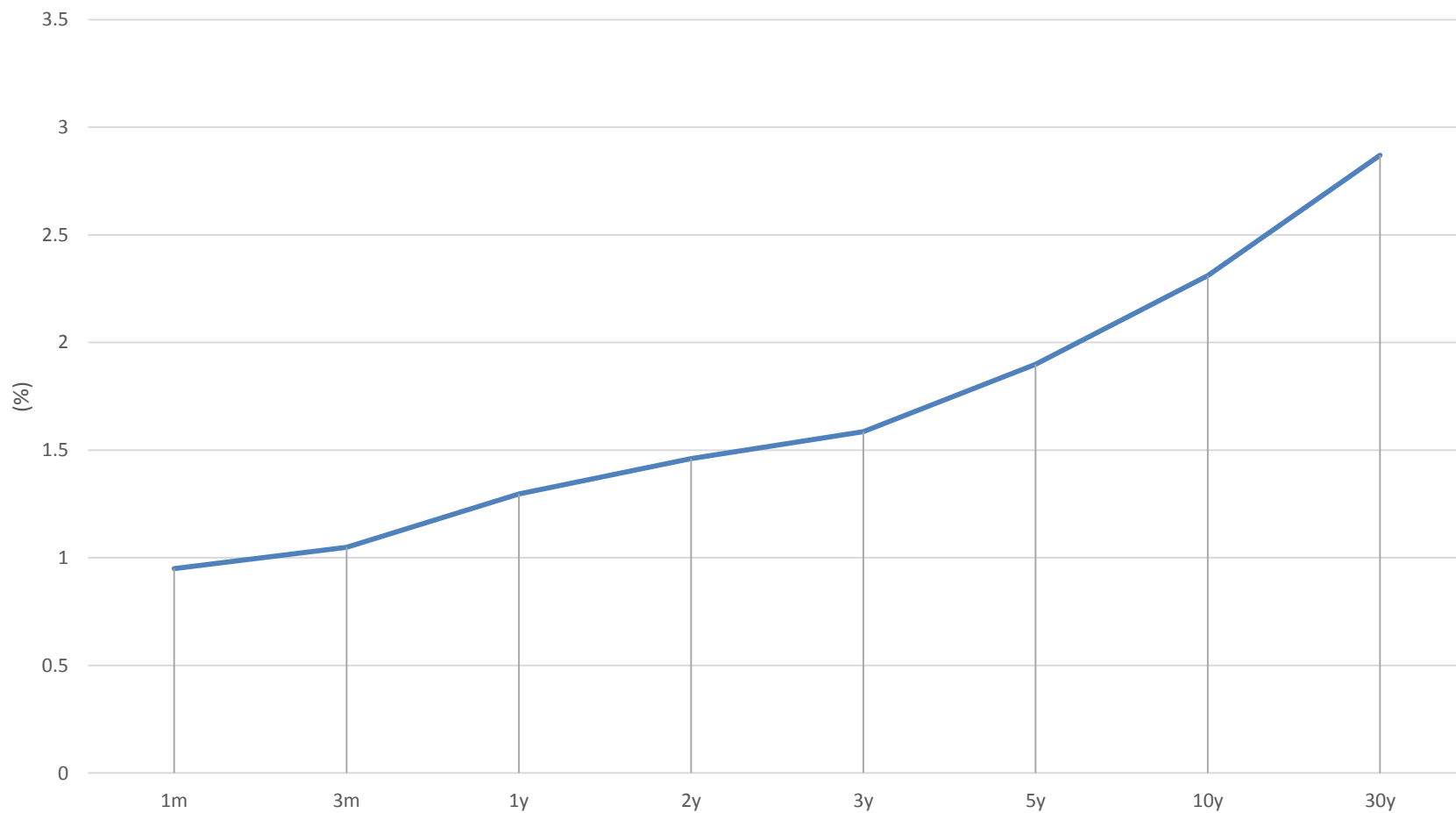
# Global Geopolitical Risks

- Rejection of Conventional Politics in 2016
- Politics – Netherlands & France OK; Germany Sept 24<sup>th</sup> OK; Italy May 2018 – cause for concern
- Migration – causing dangerous tensions in EU particularly
- Growing nationalism – Catalonia, Hungary, Poland, Austria
- Global Terrorism > North Korea, ISIS
- Trump
- Brexit
- Corporate Culture/Taxation etc

# 10-Year Bond Yields

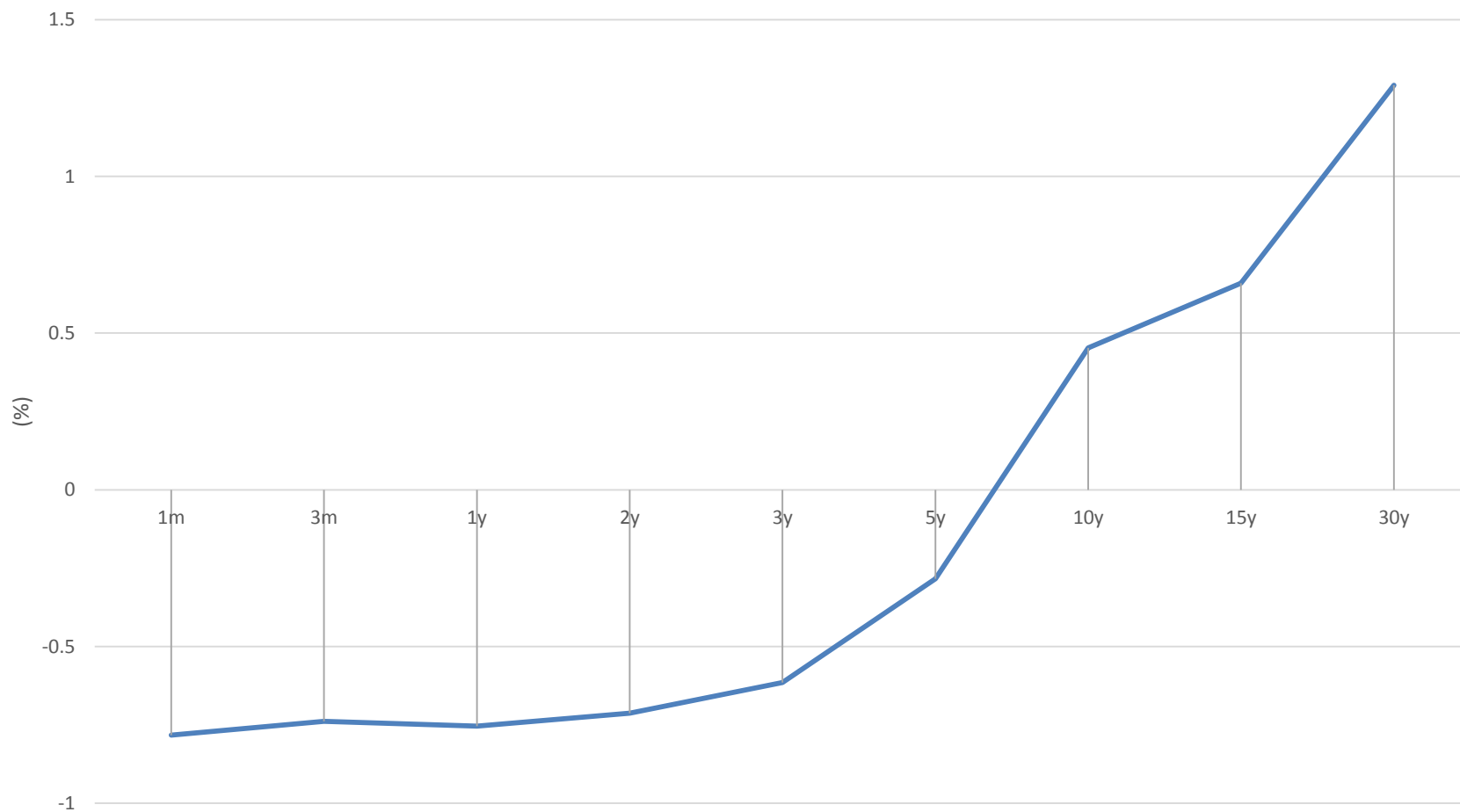
	(October 23 <sup>rd</sup> 2017)
Germany	0.43%
Ireland	0.64%
France	0.84%
Italy	2.01%
Spain	1.65%
Greece	5.52%
Portugal	2.27%
Japan	0.06%
US	2.38%
UK	1.33%

# US Yield Curve





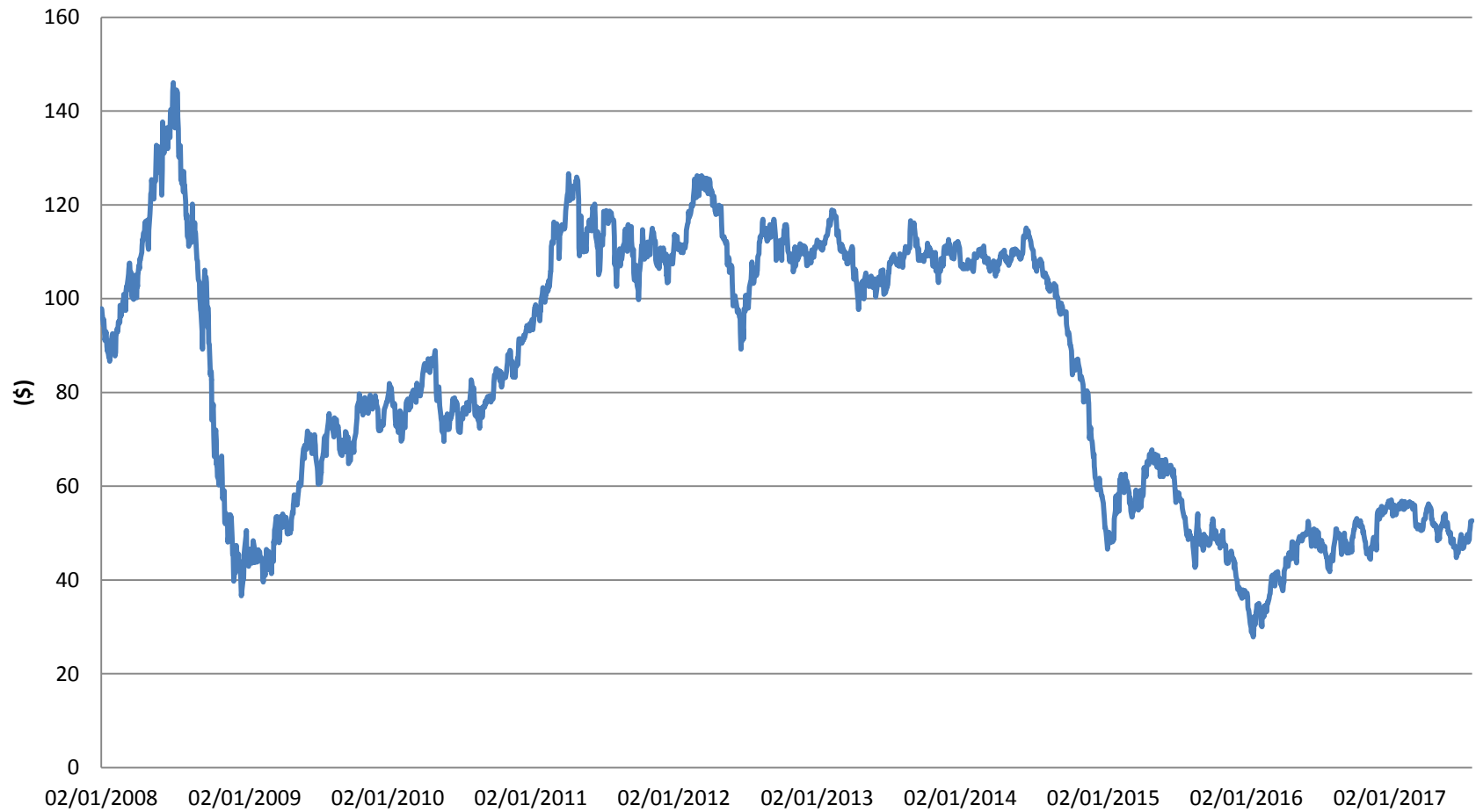
# German Yield Curve



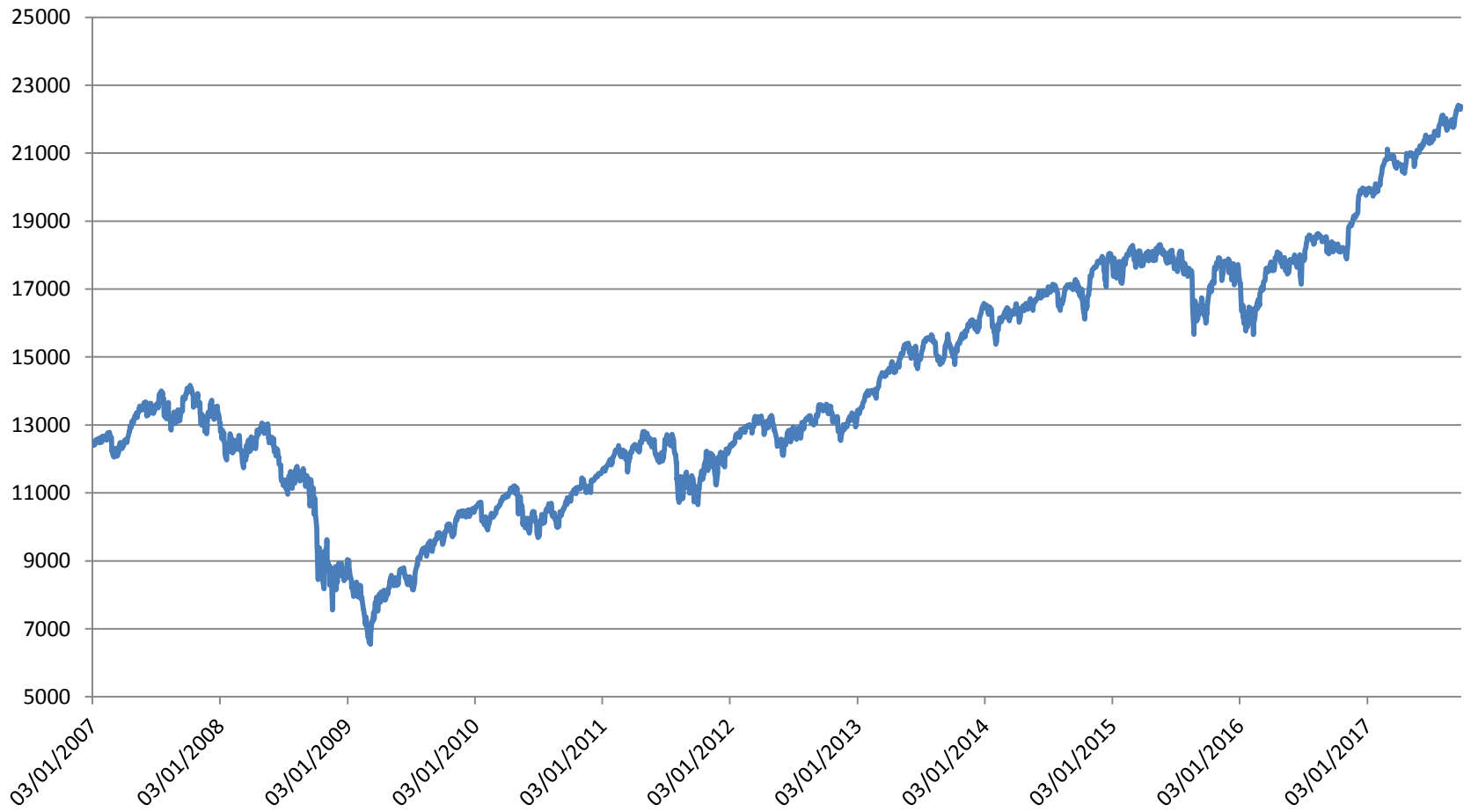
# Bloomberg Commodity Price Index



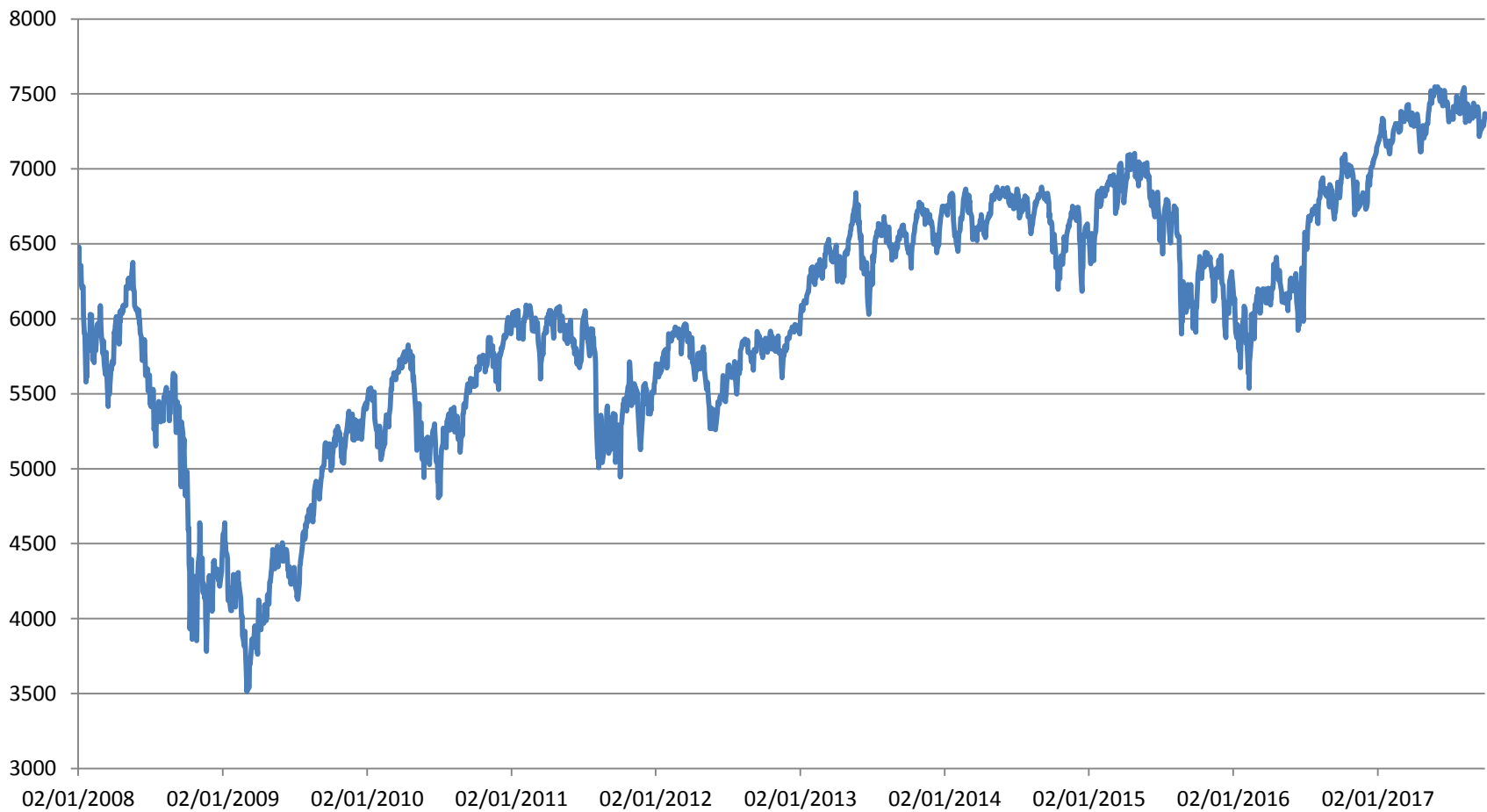
# Brent Crude Oil



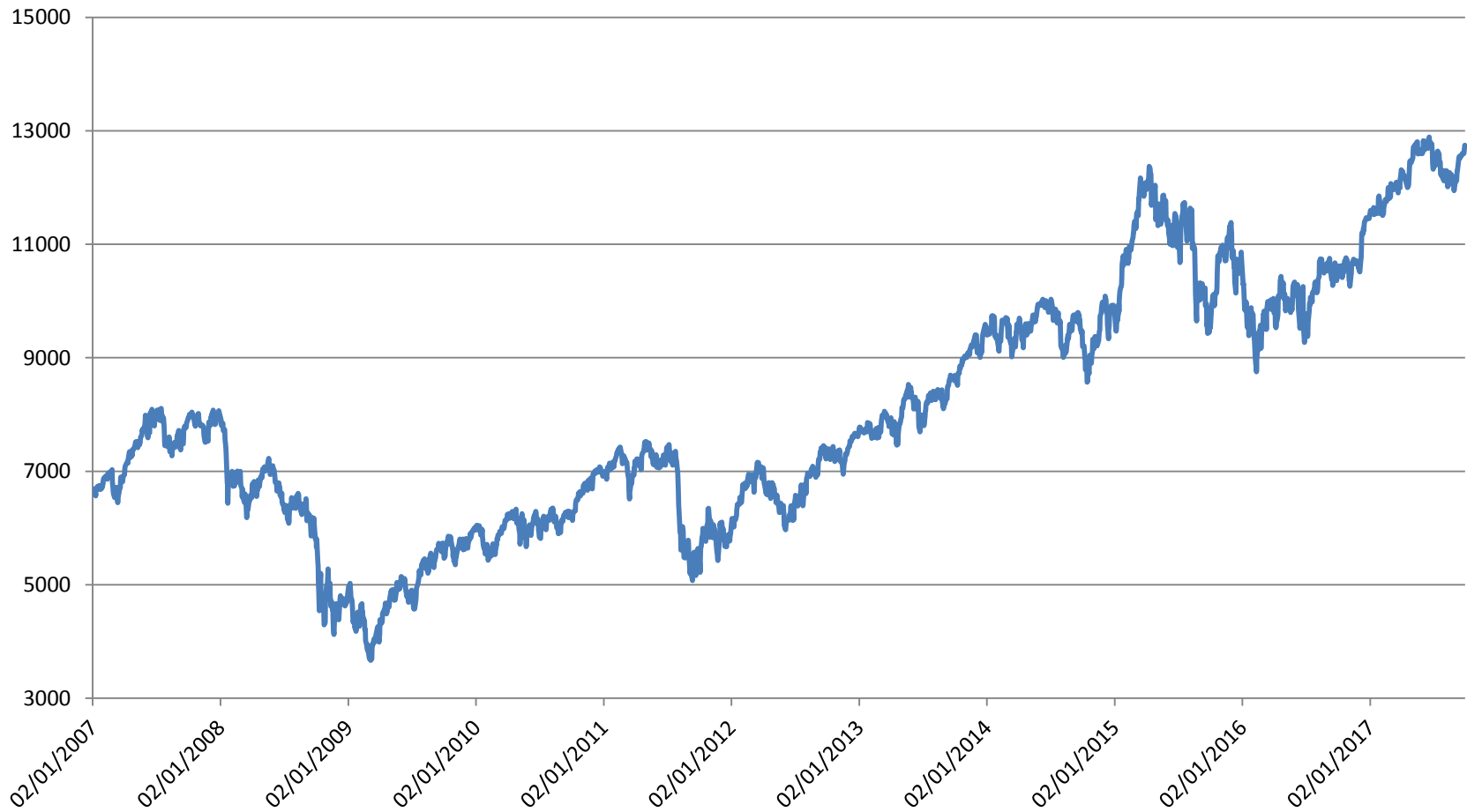
# US DJIA



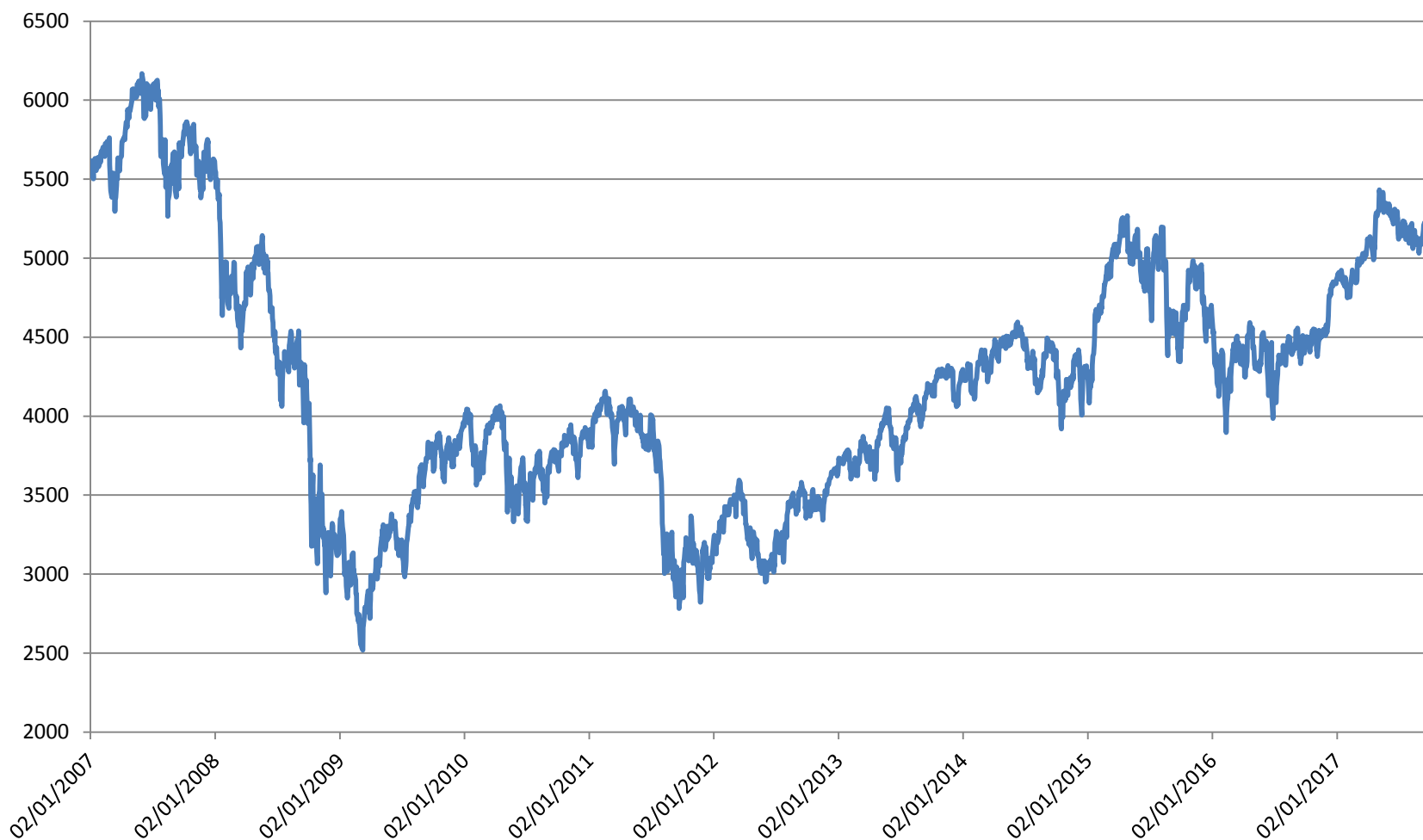
# FTSE 100



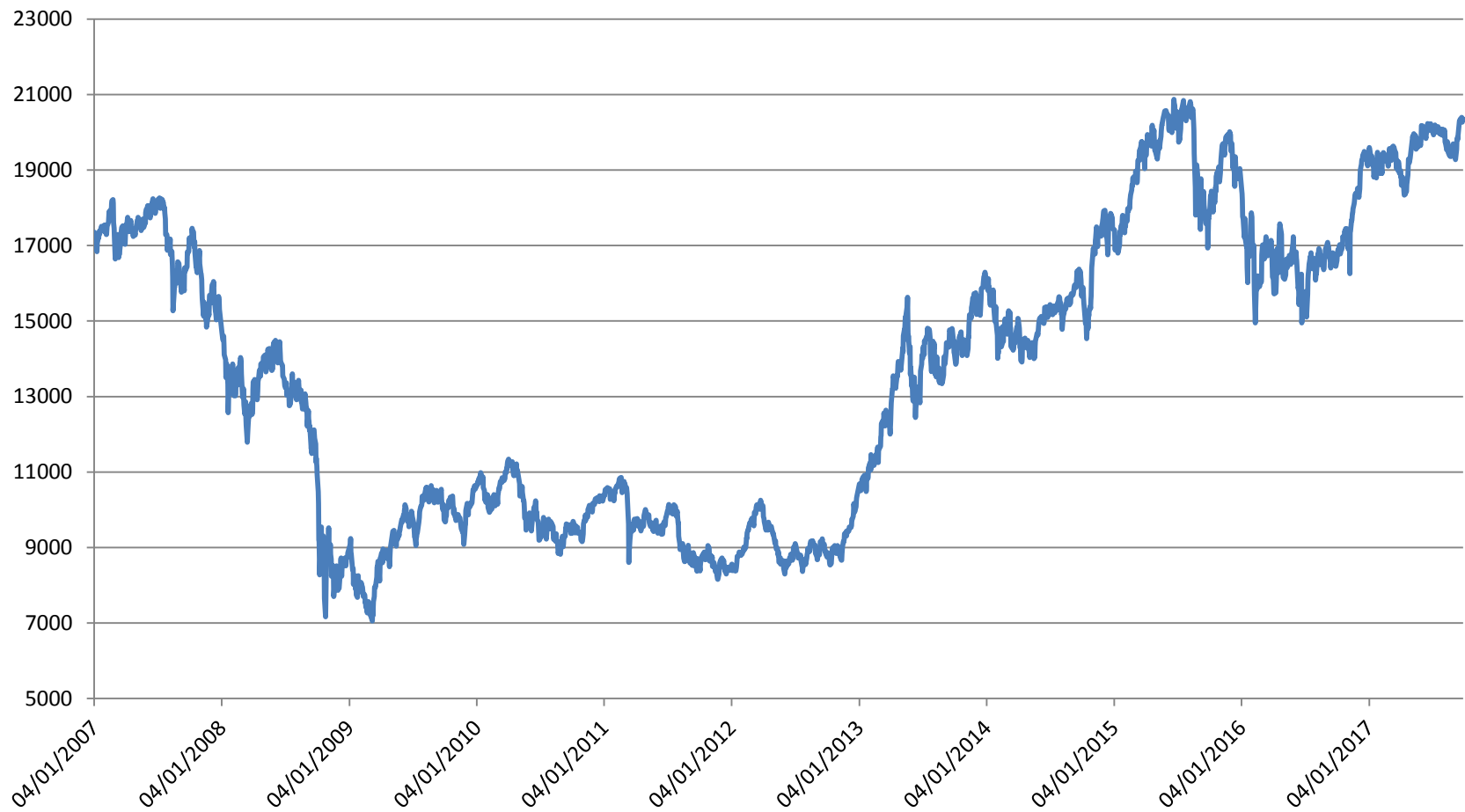
# German DAX



# French CAC

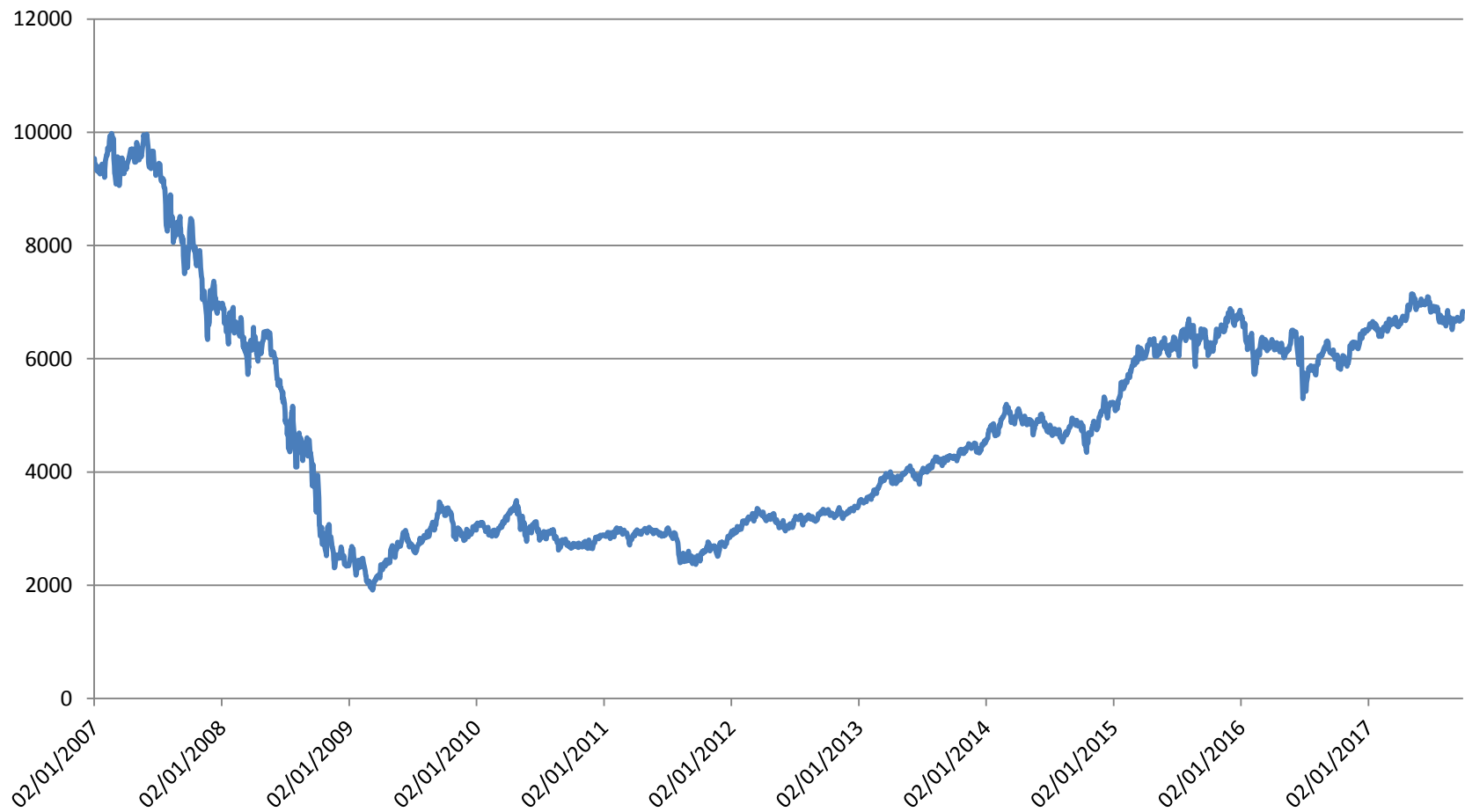


# NIKKEI





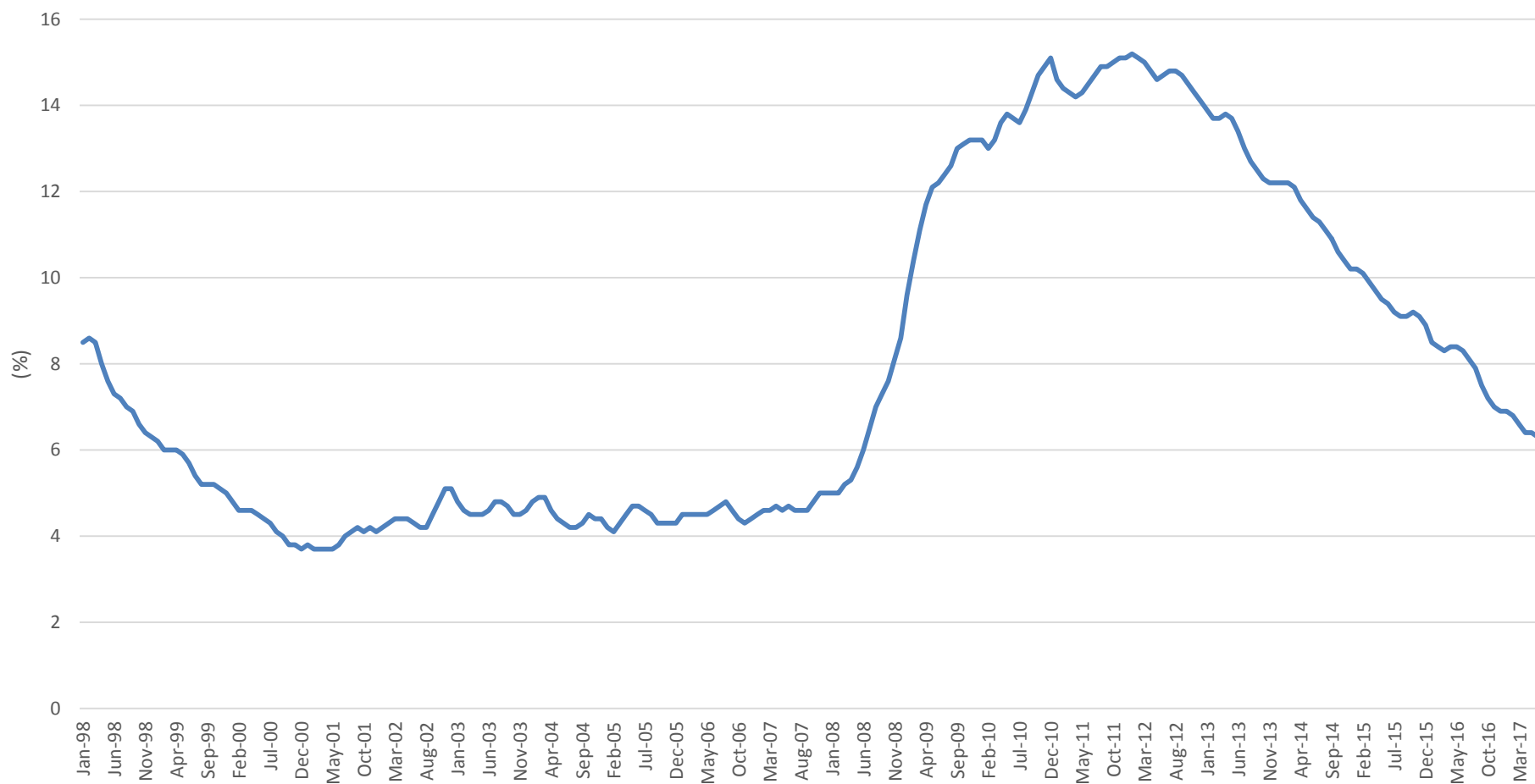
# ISEQ



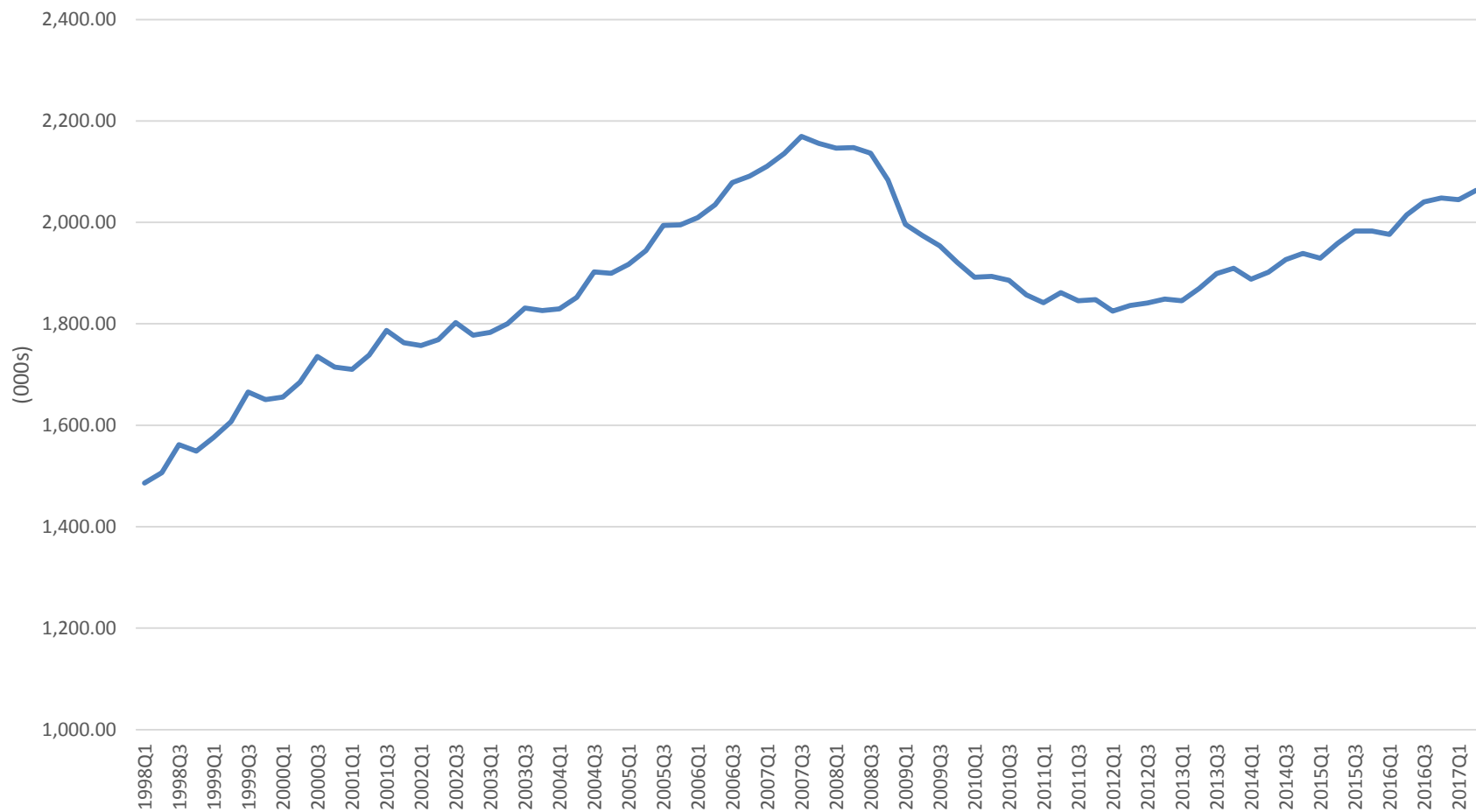
# The Irish Economy Today

- Economy in strong statistical recovery
- Significant domestic challenges
- Housing, Public Services, Pay Pressures & Pensions
- Brexit key challenge on many fronts
- Trump – tax policies
- Broader tax agendas more worrying
- Ireland needs to be managed in prudent, sensible manner
- Competitiveness broadly defined key priority

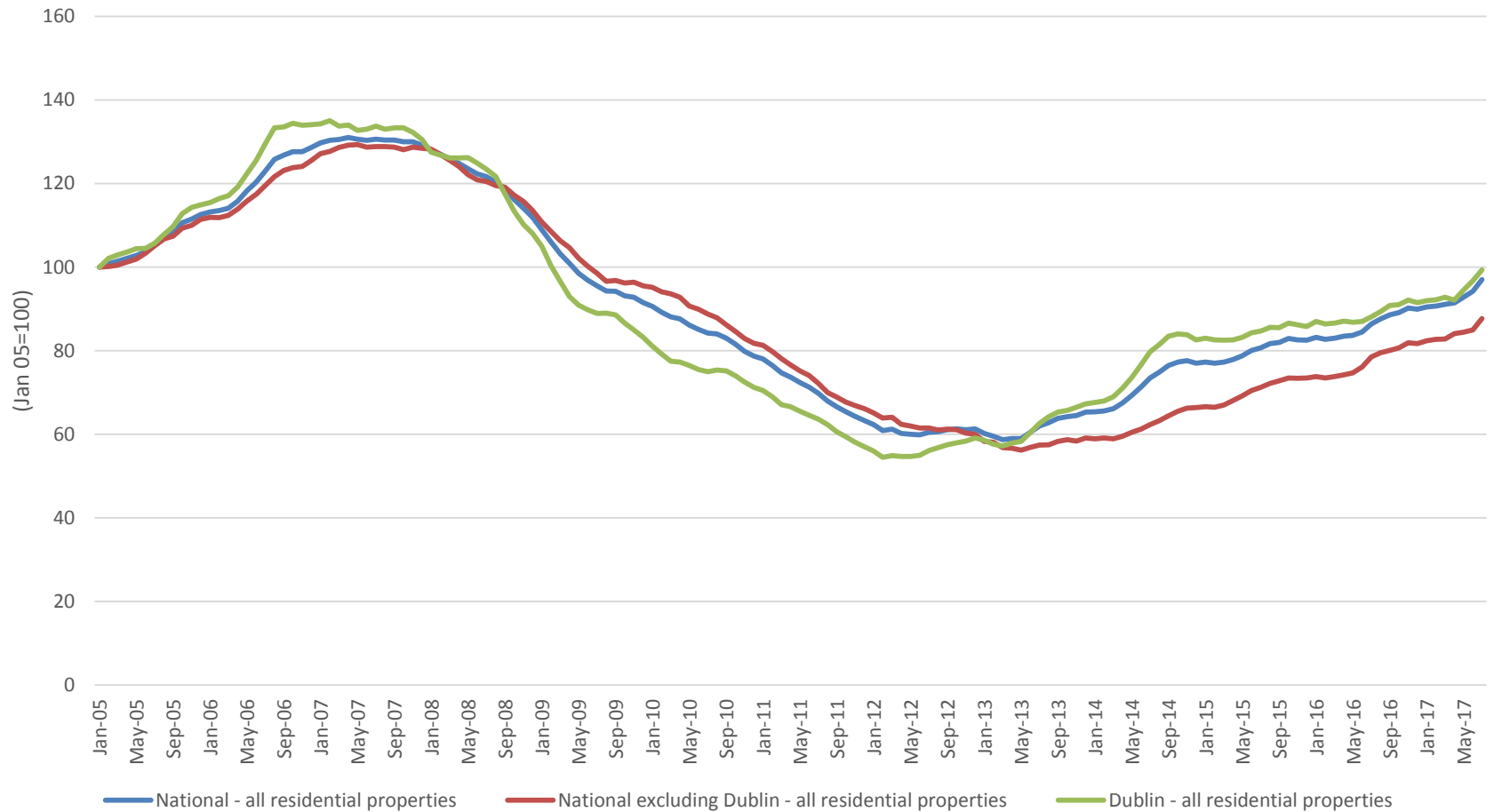
# Unemployment (% Labour Force)



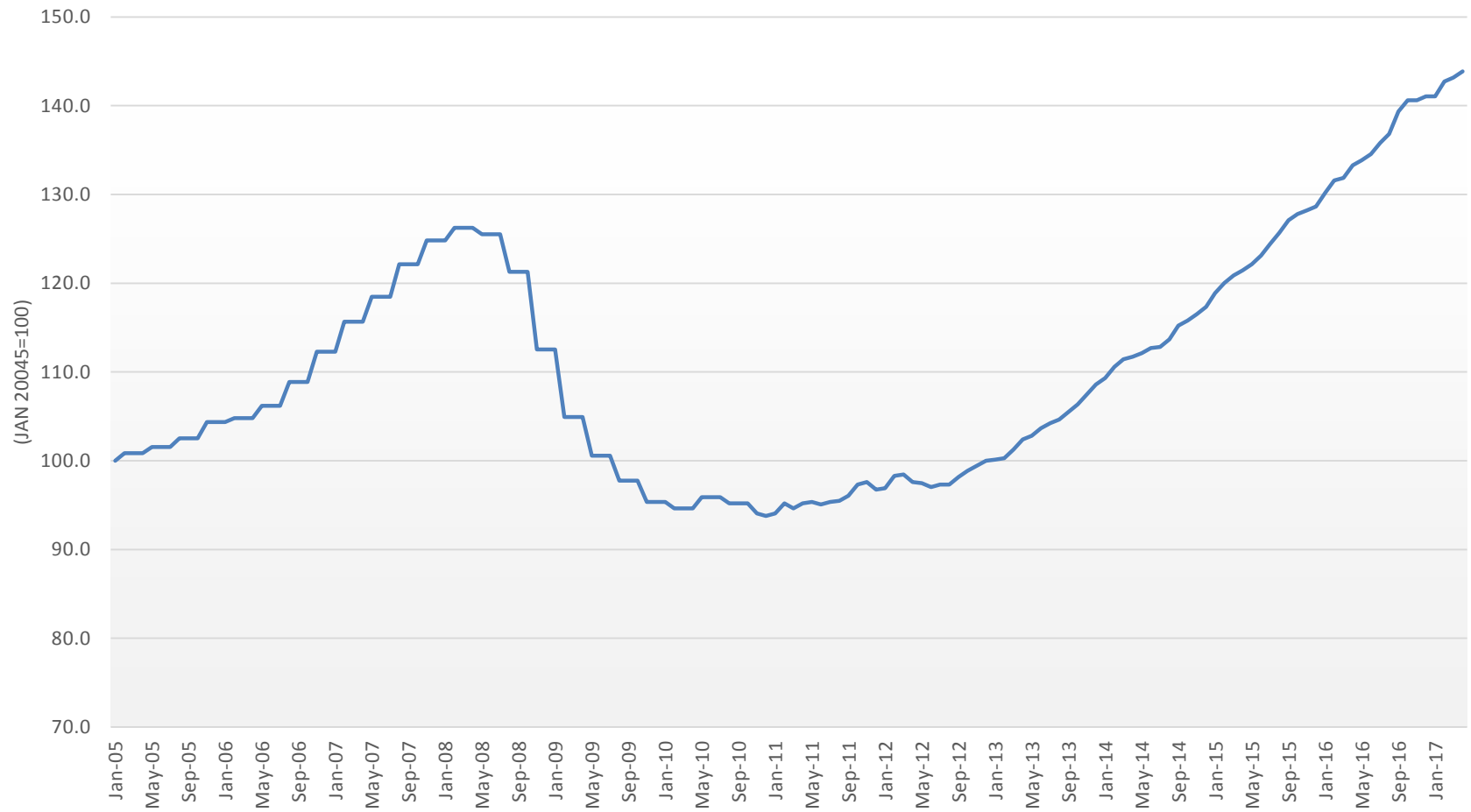
# Employment



# Irish House Prices



# Irish Private Rents



# Assumptions Budget 2018

	2017f	2018f	2019f	2020f	2017-2020
GDP	4.3%	3.5%	3.2%	2.8%	3.5%
GNP	0.0%	3.3%	3.0%	2.5%	2.2%
Consumption	2.3%	2.3%	2.2%	2.1%	2.2%
Investment	-3.7%	6.1%	5.6%	4.2%	3.1%
Government	2.0%	2.0%	2.0%	1.9%	2.0%
Exports	3.5%	4.8%	4.3%	4.0%	4.2%
Imports	-1.0	5.5%	4.9%	4.4%	3.5%
Employment	2.8%	2.3%	2.1%	1.8%	2.3%
Unemployment	6.3%	5.7%	5.5%	5.5%	5.8%

# Trends in Irish Taxation

	2006	2016	2017f	2018f
Expenditure Taxes	€19.3 bln	€18.4 bln	€19.5 bln	€20.3 bln
% Tax Take	42.4%	38.5%	38.5%	38.2%
<b>Income Tax</b>	<b>€12.4 bln</b>	<b>€19.1 bln</b>	<b>€20.2 bln</b>	<b>€21.44 bln</b>
<b>% Tax Take</b>	<b>27.2%</b>	<b>40.0%</b>	<b>39.9%</b>	<b>40.0%</b>
Corporation Tax	€6.7 bln	€7.4 bln	€7.97bln	€8.50 bln
% Tax Take	14.7%	15.4%	15.7%	15.8%
Capital Taxes	€3.5 bln	€1.2 bln	€1.2 bln	€1.31 bln
% Tax Take	7.6%	2.6%	2.5%	2.4%
<b>Total Tax Take (€bln)</b>	<b>€45.5 bln</b>	<b>€47.9bln</b>	<b>€50.6 bln</b>	<b>€53.66 bln</b>



# BREXIT – 2 ISSUES

- Currency movements Pre-Brexit
- Trading relationship Post-Brexit

# GBP v Euro



# Brexit

- Article 50 invoked by UK March 29<sup>th</sup> 2017
- EU-27 response April 29<sup>th</sup> – many conflicting aspirations
- March 29<sup>th</sup> 2019 the deadline
- UK stance complicated by domestic politics – election result has not helped
- Divorce settlement will be difficult
- 4 EU Pillars the big issue
- Terms of divorce will drive trade negotiations
- Hard Brexit the obvious risk
- 44% of UK exports to EU & 19% to US

# UK Position

- Brexit talks have stalled
- ‘Partnership and Creative Solutions’
- 3 possibilities > Norway (European Economic Area), Canada ( Free Trade Deal) & Turkey (Customs Union Arrangements)> UK has effectively ruled out all three
- 2 year transition period
- Sudden EU crash exit or compromise?

# Brexit & Ireland

- Sterling impact to date – post-Brexit trading relationship the bigger issue
- Broad & significant sectoral implications
- Trade exposure very strong > 37% Food & Drink exports; 70% Prepared Consumer Food exports go to UK
- Border Issue very problematical
- Opportunities as UK companies move to EU base – particularly financial services
- Can Ireland accommodate influx of investment?
- Housing an issue – regional opportunities

# Brexit and Ireland

- No certainty as to how the process will evolve
- Ireland has the biggest issues of the EU-27
- Every sector will be affected to varying degrees
- Legal, logistical and real economic implications
- WTO trade conditions would have profound implications for trade

# Overseas Visitors to Ireland

	2016 H1	2017H1	% CHANGE
Great Britain	1,865	1,745	-6.4%
France	263	276	+4.9%
Germany	296	309	+4.4%
Italy	158	157	-
Other Europe	812	875	+7.8%
North America	758	922	+21.6%
Australia/NZ	82	89	+8.5%
Other	150	192	+28%
Total	4,384	4,565	+4.1%

ANY QUESTIONS?





Society of Actuaries in Ireland

---

# **Integrating Risk Appetite into the Business**

---

Billy Galavan

---

# Introduction Slide

---

Billy Galavan: BAFS (1998), FSAI (2004).  
CRO, Zurich Life Assurance plc (2012).

Today's objectives:

- Outline the practical difficulties (and benefits) businesses encounter in drafting Risk Appetite Statements and embedding Risk Appetite Frameworks
- Provoke some thoughts about what a Risk Appetite Framework really represents in the business



# Recap: What is Risk Appetite?

---

- Risk appetite describes the risks to which the company is exposed and the amount of exposure it is willing to assume from those sources of risk
- Establishes boundaries for the aggregate level / types of risk a company is willing to take to achieve its objectives
- Risk appetite statements include unacceptable and preferred risks and company-wide risk tolerances
- Qualitative and quantitative dimensions, resulting in multiple ways of expressing risk appetite
- The most common group-level risk appetite statements cover:
  - Capital, earnings, liquidity, and franchise value



# The Framework: Non-negotiables

---

- Board Ownership and **Risk Strategy**
- Coverage of all risks
- Quantitative methodology (VaR, Economic Capital, Stress testing)
- Short, Medium and Long Horizons
- Regular reporting to the Board
- Appropriate breach escalation framework
- Other specific items in Corporate Governance Code:
  - Key functions
  - Remuneration and risk taking
  - Contingency planning



# Risk Strategy: Example

Risk Type	Potential Risk Strategy
<b>Insurance:</b> <i>Mortality / Morbidity / Longevity</i>	<b>Seek and manage:</b> a risk we actively want to take to deliver return / our strategy
<b>Market:</b> <ul style="list-style-type: none"><li>• <i>Liquidity</i></li><li>• <i>Matching risk</i></li><li>• <i>Equity, FX, Fixed Interest (Sovereign / Credit) and Property</i></li></ul>	<ul style="list-style-type: none"><li>• <b>Manage:</b> by-product of doing business - set capacity limits</li><li>• <b>Avoid</b></li><li>• <b>Seek &amp; manage:</b> a risk we actively want to take to deliver return &amp; strategy.</li></ul>
<b>Business:</b> <i>Expense / Inflation / Persistency</i>	<b>Manage:</b> by-product of doing business - set capacity limits
<b>Operational</b> ( <i>including Business Continuity, IT, Cyber, Info security, Third Party</i> )	<b>Tolerate and manage:</b> Operational by-product of doing business - set capacity limits
<b>Reputational</b>	<b>Avoid</b> Reputational – No Appetite
<b>Reinsurance / investment credit</b>	<b>Seek and manage:</b> a risk we want to take to deliver return



# Practical debates on Risk Appetite

---

- Concise vs comprehensive, which is more useful
  - Target Audience
- **‘Top-down’ vs ‘Bottom-up’**
  - How it should be developed?
- Subsidiary vs Group
  - Whose needs are being served?
- Firm Specific
  - ‘Off the shelf’ or bespoke?



# Top-down Approach

---

Capital & Liquidity	Earnings Volatility	Risk Behaviours
Maintain capital and liquidity levels to meet claims and regulatory / other requirements with high degree of confidence	Take sufficient (acceptable) risks to achieve target profits and cash generation in a sustainable fashion	Protect reputation and brand
Overall Regulatory Solvency Needs	New Business Value targets	Operate in line with applicable laws and regulations
Overall 'Own' Solvency Needs	'No surprises' on earnings from single sources of risk	Operate in line with Ethics Standards, Board approved Policies, Internal Controls Framework
Appropriate liquidity requirements	New Business marginal risk capital consumption	Track Key Risk Indicators



# Bottom-up Approach

			Risk Review and Scoring				
			Risk Categorisation		Inherent Risk Score		
Risk Name	Risk Description and Trigger	Risk Owner	Risk Category Level 1	Risk Sub-Category Level 2	Impact/Severity	Probability	Overall
Inadequate Staff Resourcing	<p>1. Staff Recruitment: Insufficient career planning or opportunities or salaries not being at market levels could lead to a failure to attract &amp; recruit experienced and highly skilled staff.</p> <p>2. Staff Retention: Insufficient career planning or opportunities or salaries not being at market levels could lead to loss of experienced, highly trained or high talent staff</p>	Manager X	Operational Risk	People Management	Low €0 - €10m	It will happen sooner or later (28%-63%)	Low-High
Fraud - Internal & External	<p>1. The risk of fraudulent Med Fee payments being made as a result of inadequate controls, resulting in a financial loss for the company.</p> <p>2. Risk of fraudulent business being placed on cover through inadequate controls. (By customer or by Broker via non disclosure)</p> <p>3. Potential for internal fraud to occur through inadequate controls, resulting in a financial loss for the company. For example, fraudulent expenses, misuse of delegated authorities etc.</p>	Manager X	Operational Risk	Fraud	High - Regulatory Issue/Adverse Media Attention	It shouldn't happen but is possible (3%-10%)	High-Very Low





# Helpful tips in framework design

---

- **Common language** – invest time in this!
- Definition – FSB definition appears to be more widely accepted
  - *The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan*
- Can't design it all in one go or lift straight off the shelf:
  - Construct the framework (roles and responsibilities)
  - Document the Statement (Range of risks)
  - Calibrate the limits (Only once relevant risks have been fully agreed)



# Common Language



<b>Risk Appetite</b>	The aggregate level and types of risk a firm is willing to assume within its risk capacity to achieve its strategic objectives and business plan
<b>Risk Capacity</b>	The maximum level of risk the firm can assume before breaching constraints determined by regulatory capital and liquidity needs and its obligations, also from a conduct perspective, to depositors, policyholders, other customers, and shareholders
<b>Buffer</b>	One issue is how big the buffer between appetite and capacity should be. The buffer should consider possibility of very extreme outcomes and modelling error
<b>Risk tolerances</b>	Quantitative measures and qualitative assertions for maximum risk allowed by appetite. They should be measurable and reported and monitored by the Board and senior management



# Helpful tips in embedding

---

- **'Cheat sheet'** for everyday use:
  - Risk type
  - Metrics in use
  - Applicable policies
  - Responsible roles and relevant Governance Fora
- Projections of compliance with Risk Appetite are a necessary requirement in signing off on a business plan
- New product launches and product reviews need to incorporate Risk Appetite compliance
- Be explicit! Branding all material limits under the 'Risk Appetite' banner will attach a degree of rigour that might otherwise not exist.



# 'Cheat sheet'

Illustrative Mind Map	Aggregate Level	ALM, Investment & Credit Risk	Life Liability Risks & Reinsurance Credit Risk	Business Risks	Operational Risk	Reputational Risk
Policies	Risk Management Policy Audit Policy Capital Policy Remuneration Policy Concentration Risk Policy	ALM Policy Investment Policy Liquidity Policy	Reserving Claims U/W Reinsurance	Expense Policies Retention Policies	Outsourcing Business Continuity Information Security	Compliance Policy F&P Policy Conflicts of interest Reputational Risk
Committees	Board Board Risk C'tee Risk and Control C'tee Product Development C'tee	ALM and Investment C'tee	U/W C'tee, Claims C'tee, Reinsurance C'tee	Audit C'tee	Information Governance Outsourcing Oversight Operational Risk C'tee	Board Audit C'tee Assurance Coordination
Persons (Management)	CEO CRO Head of Capital Management	CFO Chief Investment Officer	HoAF Chief underwriting Officer Head of Claims	CFO Chief Operating Officer	Chief Operating Officer	CEO Compliance Officer
Measures	Solvency Economic Capital Risk Dashboard	Economic Capital Stress Tests Investment Guidelines	Economic Capital Stress Tests	Economic Capital Stress Tests	Operational Risk Capital Operational Risk KRIs	Breaches Complaints Controls Effectiveness Audit Outcomes
Activities / Reports	Risk Register (RCSAs) ORSA Emerging Risks	Stress testing Investment Guideline Compliance Reports Concentration Risk Reports	Suite of Actuarial Function Reporting Assumptions review	Assumptions review, GLER, Lapse Reporting	IT Risk Reportings Loss Events Reporting RCSA	Breaches Complaints Controls Effectiveness Audit Outcomes
Controls	Operational Controls Financial Controls Economic Capital Controls Compliance with Laws & Regs	Operational Controls Financial Controls Economic Capital Controls Compliance with Laws & Regs	Operational Controls Economic Capital Controls	Operational Controls Financial Controls	Operational Controls IT Standards	Operational Controls Compliance with Laws & Regs



# Key Benefit: Guidance on business decisions

---

- **Integral part of Strategy, Business Planning and ORSA**
- This drives Capital Management – Risk and Capital Optimisation
- Day to day decisions throughout the year consistent with strategy and plan are guided by Risk Appetite (and KRI tracking):
  - Product profitability and suitability reviews
  - Investment Committee asset allocation decisions
  - Reinsurance decisions
  - Outsourcing reviews
  - Employee turnover



# Integrated approach

---





# Useful information

---

- Principles for an Effective Risk Appetite Framework – FSB 2013
- Risk Appetite: A discussion paper – CBI 2014
  - Presentation from Máiréad Devine & John McElligott to the SAI ERM Forum on 14th April 2015 titled ‘Risk Appetite Perspectives from the Central Bank of Ireland’
- 2013 SAI Risk Insights conference presentation by Eamonn Phelan titled ‘Risk Appetite – Latest developments’
- ERM Database: SAI Working Party paper from March 2011 ‘Constructing a Risk Appetite Framework: an Introduction’



Society of Actuaries in Ireland

---

**Questions?**

---

Billy Galavan, 25<sup>th</sup> October 2017

---





# Risk Communication

An introduction on how to  
better interact with your  
business partners

by Caroline Grégoire

Dublin, 25 October 2017

## With Risk Communication...

### ... WE OFTEN UNDERSTAND AND REFER TO:

- Various written communication, e.g. reports, guidelines, e-mails, meeting minutes, etc.
- Various presentations/discussions held during board meetings, risk management workshops, etc.

### ... AND IT ALSO INCLUDES...

- Informal talks in the cafeteria, when leaving a meeting, during a coffee break...

The challenge: a wide variety of stakeholders with different degrees of understanding and acceptance of the actuarial/risk management issues or terms

Introduction

Risk Communication

25 October 2017

Let's start!

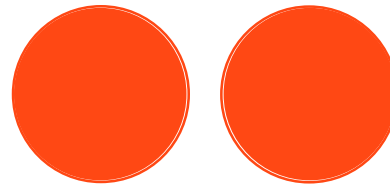
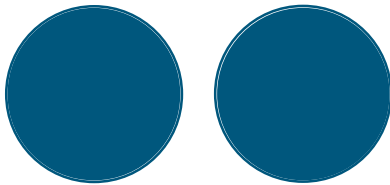
A asks B:

WHY DID YOU CHOOSE YOUR CURRENT JOB?

B answers during **2 minutes** while A listens

**AND CHANGE ROLES** (A <-> B)

B asks the question, A answers during **2 minutes** while B listens



Introduction

Risk Communication

25 October 2017

# 4 types of listening

0: no listening

1: „internal“ listening

2: „external“ listening

3: listening for patterns...

# Pattern No. 1

## PROCEDURE / ALTERNATIVE: EXAMPLE OF USED WORDS/EXPRESSIONS

### PROCEDURE

- first... second...
- step by step
- at the end
- process
- the best way
- method

### ALTERNATIVE

- possibilities / options
- to choose
- a better way
- a list of criteria

Pattern no. 1

Risk Communication

25 October 2017

## Exercise: person A and person B

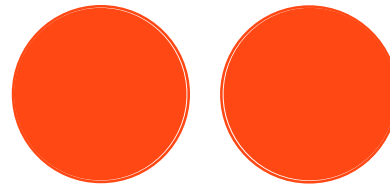
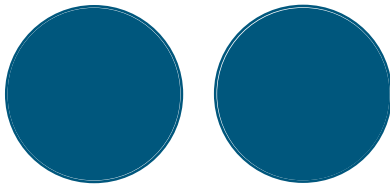
A asks B:

### HOW DOES YOUR OFFICE LOOK LIKE?

B answers during **2 minutes** while A listens

**AND CHANGE ROLES** (A <-> B)

B asks the question, A answers during **2 minutes** while B listens



Pattern no. 2

Risk Communication

25 October 2017

## Pattern No. 2

### OVERVIEW / DETAILS: EXAMPLE OF USED WORDS/EXPRESSIONS

#### OVERVIEW

- purpose
- summary
- concept
- „the idea is...“
- „the most important is...“
- simple sentences and few details
- information often not in a specific order

#### DETAILS

- use of many adverbs and adjectives
- correct names of persons / places
- concrete information
- information provided often linear
- „exact, specific“

Pattern no. 2

Risk Communication

25 October 2017

## Exercise: person A and person B

A asks B:

**WHY IS IT IMPORTANT FOR YOU TO: EXERCISE?**

B answers: Answer 1

2. A: WHY IS IT IMPORTANT FOR YOU TO Answer 1 ? B: Answer 2

3. A: WHY IS IT IMPORTANT FOR YOU TO Answer 2 ? B: Answer 3

And continue until the WHY question was asked 5 times...

**AND CHANGE ROLES** (A <-> B)

Pattern no. 3

Risk Communication

25 October 2017



## Pattern No. 3

### TO / FROM: EXAMPLE OF USED WORDS/EXPRESSIONS

#### TO or TOWARDS

- want to have / reach
- focus on goal / results
- to make it happen
- to start
- to win
- to do / make more
- to include (people, things, places)

#### (AWAY) FROM

- don't want to have
- to avoid / prevent
- to solve problems
- to do / make less
- to exclude

Pattern no. 3

Risk Communication

25 October 2017

## 3 key take-aways

### 1. LISTEN for PATTERNS (remember: situation-specific, please no label!)

- procedure / alternative
- overview / details
- towards / away from

### 2. USE THE PATTERNS OF YOUR BUSINESS PARTNERS to make a better impact with your message

- Adapt the „how“ of your communication, the „what“ remains the same

### 3. CHOOSE your MINDSET! Like:

- Positive, calm, constructive, enthusiastic, open, etc. (as long as it aligns with the intention of connecting with those you communicate)

Key take-aways

Risk Communication

25 October 2017

## A Conclusion...

... I WISH YOU ALL THE BEST IN YOUR FUTURE  
... SO THAT YOU CAN MINIMISE THE

## RISK COMMUNICATION

Conclusion

Risk Communication

25 October 2017



Contact: [caroline.gregoire@cg-four.com](mailto:caroline.gregoire@cg-four.com)

Interested to learn more? [www.cg-four.com/en](http://www.cg-four.com/en)

Search for „Actuaries on stage“



Society of Actuaries in Ireland

---

# **Recovery and resolution plans in banking**

---

**Monika Smatralova**

---

# Introduction

---

## **Focus of today's presentation:**

- A brief summary of the latest developments regarding recovery and resolution for (re) insurers.
- An overview of the building blocks and challenges facing banks in the preparation and delivery of the Recovery and Resolution Plans and what key lessons may be learnt from it.



Dr Monika Smatralova is a senior risk practitioner currently leading the Supervisory Review and Evaluation Process within Group Risk, Permanent tsb. Her academic background is in 'Financial Management'. She has been working in risk functions of major high street and captive banks for the last 10 years focusing mainly on credit and operational risk management and measurement, and Enterprise risk management.

Monika is also actively involved in the senior leadership at PRMIA, successfully leading the Irish Chapter since 2013. In 2014 she was elected as the EMEA Regional Directors Committee Co Chair and member of PRMIA Global Council. In 2015 Monika joined the PRMIA Educational Committee. She is a co-author of the PRM designation text books and has published articles in various technical magazines and journals.



# Recovery and Resolution for (Re) Insurers

*No formal requirements for recovery and resolution plans in Ireland for (Re) Insurers.*

## Current requirements for large companies

- G-SIFIs must undertake recovery and resolution planning
- IAIS requirements adopted for Global Systemically Important Insurers (G-SIIs), Includes 5 EU insurance groups: **Aegon N.V., Allianz SE, Aviva plc, Axa S.A. and Prudential plc**

## PRA's Fundamental Rule 8 is for all insurance companies to have a resolution plan

- No current plans to issue guidance

## EIOPA Opinion – Recovery and Resolution Framework

Building Blocks	
1. Preparation and planning	Pre-emptive recovery planning
	Pre-emptive resolution planning
	Resolvability assessment Early intervention
2. Early intervention	Early intervention conditions
	Early intervention powers
Recovery	Solvency II ladder of intervention – out of scope Resolution
3. Resolution	Resolution authority
	Objectives, Conditions, Powers, Safeguards
4. Cooperation and coordination	Cross-border cooperation and coordination arrangements

EIOPA have called for a harmonised recovery and resolution framework for all (re)insurers in July 2017 following a qualitative assessment and consultation:

- Minimum harmonisation
- Recovery plans
- Early intervention powers not a new capital requirement
- Resolution powers – aim to preserve value
- A natural extension of the ORSA and contingency planning, which are a source of input



- Established by Regulation (EU) No 806/2014 on the Single Resolution Mechanism (SRM Regulation), the Single Resolution Board (SRB) has been operational as an independent European Union (EU) Agency since January 2015.
- 2017 is the third year of drafting recovery plans for banks.
- And it is **still evolving on both sides...**
- Resolutions Plans are drafted by the regulator and only partially shared with the banks.







# Elements of Recovery Plans

---

“Banks should develop recovery plans that identify credible options to survive a range of severe but plausible stressed scenarios.” Regulator

## ***Key Building Blocks :***



1. Governance



2. Documentation and Data



3. Integration



4. Scope



5. Critical functions



6. Recovery Plan Indicators & Triggers



7. Recovery Options



8. Scenarios



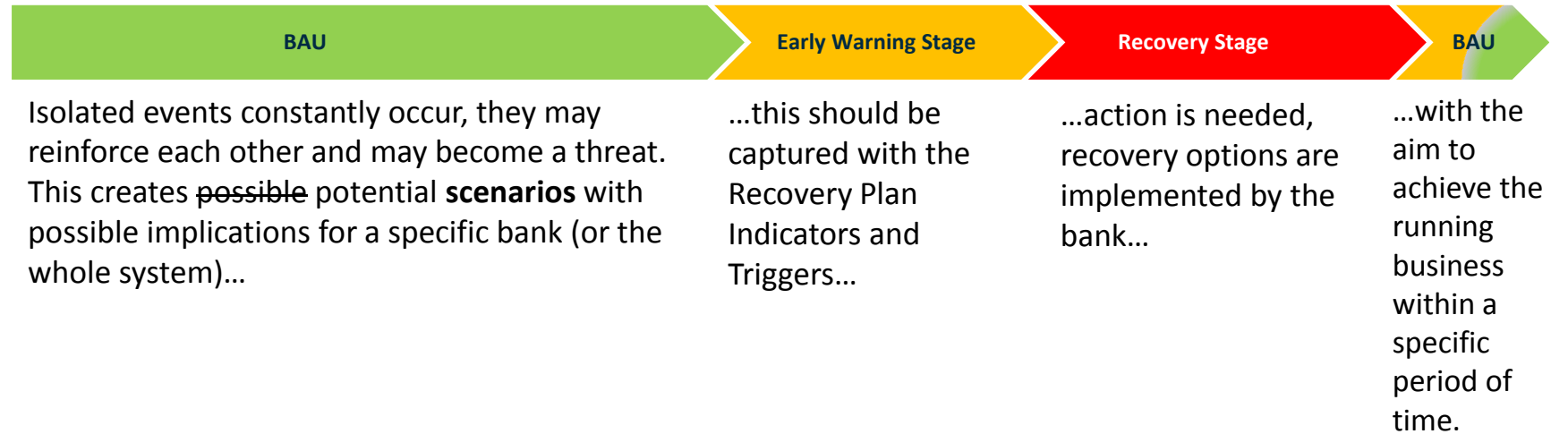
9. Testing, feasibility and updating




10. Communication



# So how it works practically....



Scenarios	Indicators	Recovery Measures/Options	Indicators
Idio-syncratic (fast)	Impact 	<div>12 months</div> <ul style="list-style-type: none"> <li>➤ Capital Raising &amp;/or Preservation</li> <li>➤ Restructuring of Liabilities</li> <li>➤ Cost Reduction</li> <li>➤ Sale of Assets/Loan Portfolio</li> <li>➤ Liquidity Improvement Recovery</li> <li>➤ Reduction of RWA/Leverage</li> <li>➤ Disposal Recovery Options</li> <li>➤ Management Actions</li> </ul>	Back to 'Normality'
Market-wide (fast)	Impact		
Idio-syncratic (gradually, slow)	Impact		
Market-wide (gradually, slow)	Impact		
Combo – Idiosyncratic & market –wide (fast)	Impact		
Combo – Idiosyncratic & market – wide (gradually, slow)	Impact		



# Example: Recovery Options in Banking

Awareness of the logistics of execution and its impediments is crucial.

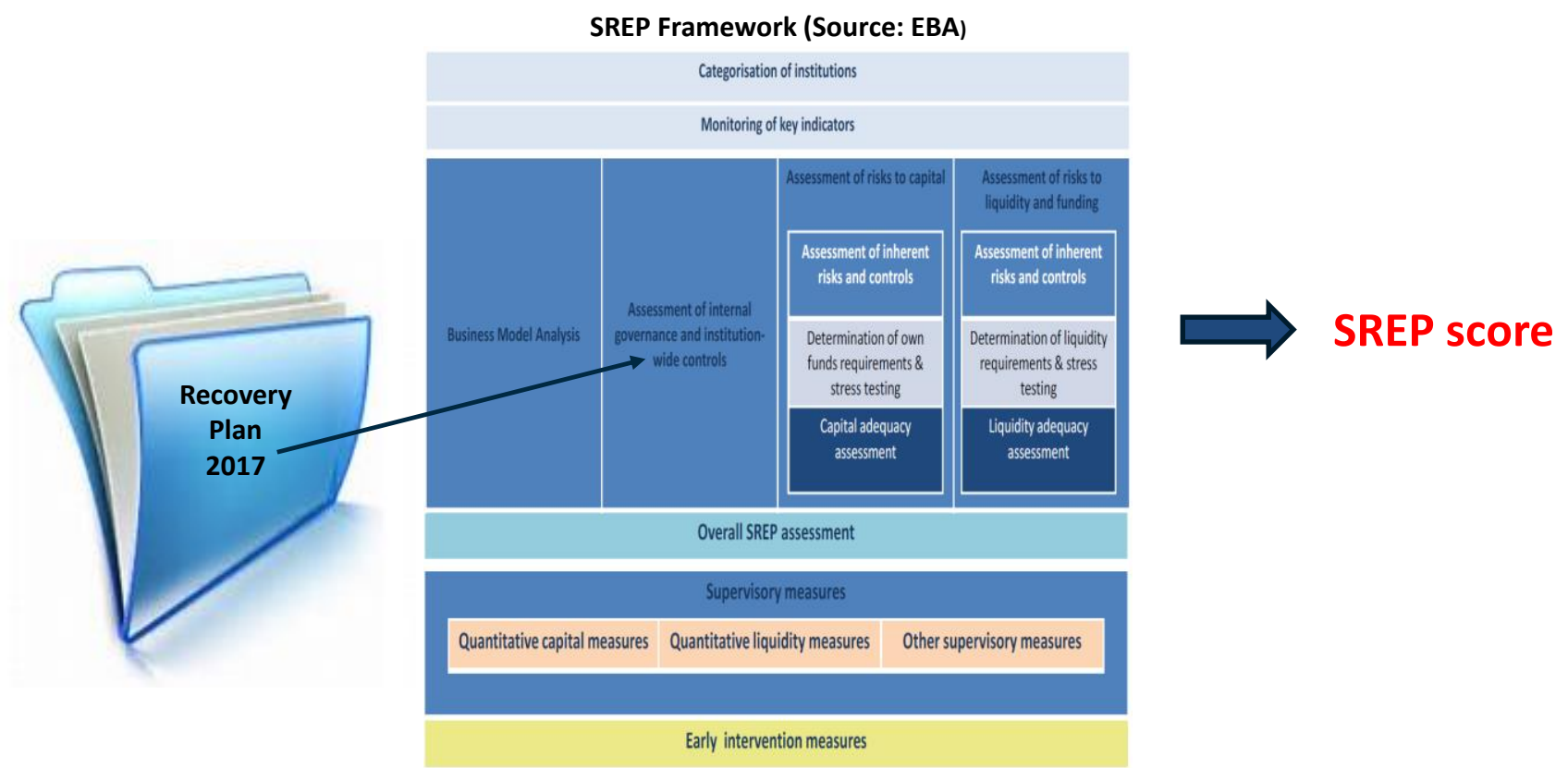
Capital Raising	Capital preservation	Restructuring of liabilities	Sale of asset/loan portfolio	Liquidity Improvement	Reduction of RWA/leverage	Disposal Recovery Options	Management Actions/Cost Reductions
<ul style="list-style-type: none"> <li>➤ Rights issue</li> <li>➤ Ordinary capital increase</li> <li>➤ Issue of mandatory convertible bond</li> <li>➤ Issue of AT1</li> <li>➤ Issue of T2</li> <li>➤ Parent support</li> <li>➤ Conversion of T2 capital into T1 capital</li> <li>➤ Intra-group credit line</li> </ul>	<ul style="list-style-type: none"> <li>➤ No distribution of dividends to shareholders</li> <li>➤ No payment of coupon on AT1/T2 issues</li> <li>➤ Earnings retention</li> </ul>	<ul style="list-style-type: none"> <li>➤ Liability management transactions</li> <li>➤ T2 instruments buyback</li> <li>➤ Reduce the trading book</li> <li>➤ Organic loan portfolio reduction</li> </ul>	<ul style="list-style-type: none"> <li>➤ Sales of leveraged loan portfolios</li> <li>➤ Securitisation of portfolios</li> <li>➤ Synthetic securitisation</li> <li>➤ Asset sales – real estate</li> </ul>	<ul style="list-style-type: none"> <li>➤ Retained covered bonds</li> <li>➤ Accessing central bank liquidity facilities with routine collateral</li> <li>➤ Repo or pledge high-quality liquid assets</li> <li>➤ Replace, sell, repo or swap non-high-quality liquid assets</li> </ul>	<ul style="list-style-type: none"> <li>➤ Unwind of portfolio management</li> <li>➤ Unwind of fixed income financing</li> <li>➤ Portfolio run-off</li> <li>➤ Sale of strategic equity stakes</li> <li>➤ Unwind of equity derivatives business</li> </ul>	<ul style="list-style-type: none"> <li>➤ Sale of business lines</li> <li>➤ Sale of subsidiaries</li> <li>➤ Sale of significant equity holdings</li> </ul>	<ul style="list-style-type: none"> <li>➤ Reduction in personnel</li> <li>➤ Stop/delay IT investments</li> <li>➤ Cancel bonus payment</li> <li>➤ Reduction in working time</li> <li>➤ Reduce lending</li> <li>➤ Increase fee income</li> </ul>

**The selection of the appropriate option (s) depends on the severity and characteristics of the risk event, options may be combined in order to support the bank's return to the BAU status.**



# Regulator assesses the Bank's Recovery Plan

Recovery plan is assessed under the Supervisory Review and Evaluation Process (SREP) and therefore impacts the Bank's SREP score.





# Recovery Plans – Practical Experience

---

- Intended to be living documents which demonstrate that the recovery measures presented can be implemented in reality – and that is not an easy task (superficial plans are rejected, resubmissions are required)
- Must be achievable (practical) and capable of being put into action straight away (executed within 12 months)
- Consideration for Idiosyncratic vs systemic situations or both (fast vs slow pace)
- Operational plans (levering with existing contingency planning) – arranging counterparties, setting up data rooms, line up investment banks etc.
- Consistency with ICAAP, Risk Appetite Statement and Stress Testing/Risk Management (existing Risk Management Framework)
- A number of iterations are required as regulator and company evolves expectations of plans
- Resolution plan not typically disclosed to the bank
- The length of recovery plans can span hundreds of pages, maintenance of the plan, data and supporting analysis is a crucial requirement
- Synchronisation of the Operational and Financial Contingency
- Interpretation of the regulations – potential inconsistency in regulatory requirements and possible national interests



# Case Study: recent cases

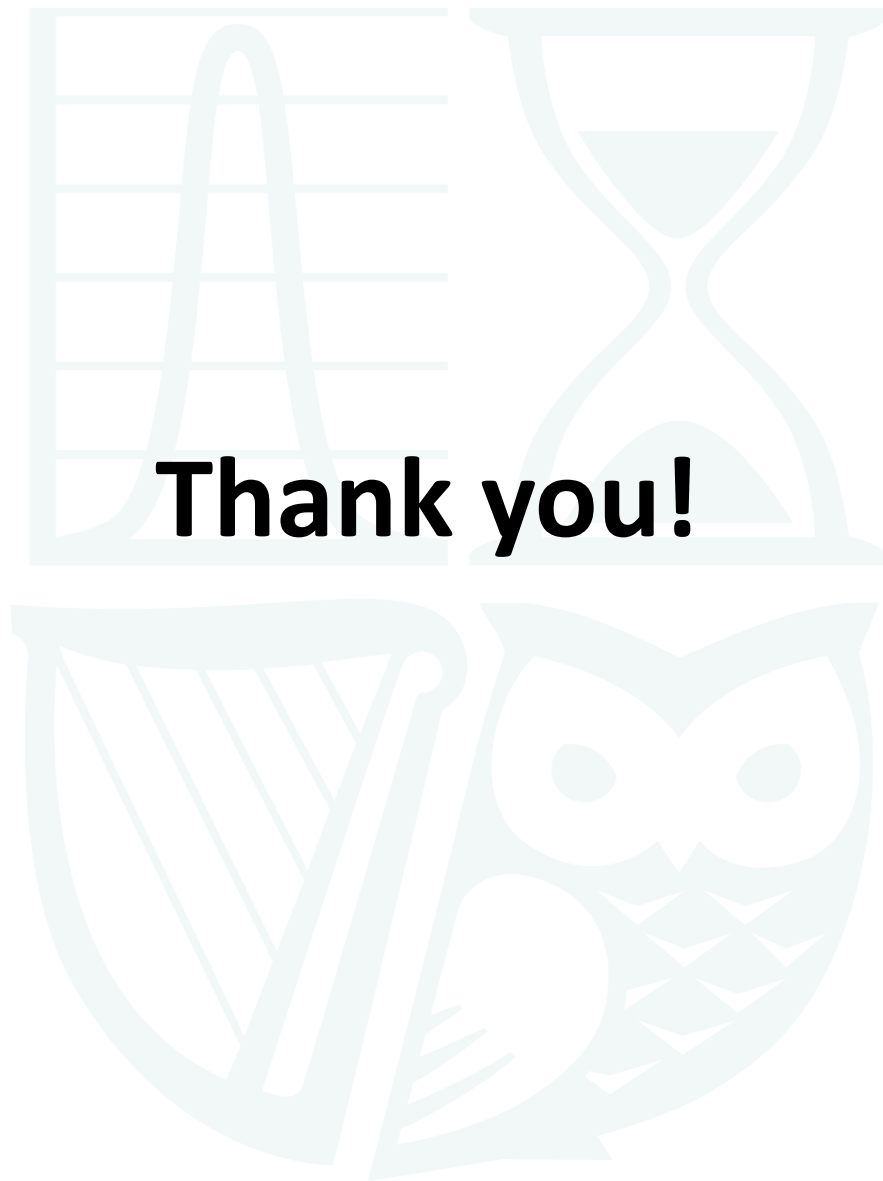
---

## **Banco Popular Español S.A. (7 June 2017, Spain)**

- Driven by a significant deterioration of bank's liquidity situation (approx. €2bn withdrawn a day)
- Collapse primarily attributed to 'toxic' real estate loans on its books and its failure to raise fresh capital
- SRB assessed that the resolution of bank is in the public interest and adopted a resolution scheme
- Shareholders and junior bondholders have been wiped out

## **Veneto Banca & Banca Popolare di Vicenza (25 June 2017, Italy)**

- Driven by bad loans and dragged down by a mis-selling scandal
- Decision a result of lack of capital (failed attempts to raise fresh capital)
- SRM concluded that conditions for a resolution action were not fulfilled
- Banks to be wound up under Italian insolvency procedures (a total cost of up to €17bn)



**Thank you!**



Society of Actuaries in Ireland

---

# **General Data Protection Regulation: Legal Insights and Impact on Insurers**

---

Paul Lavery

---



# Topics

---

- The EU Data Protection Regulation – Main Prospective Changes
- Impact on (Re) Insurers
- Countdown to Compliance



# Existing legislative Regime

---

- Data Protection Acts, 1988 and 2003
- Data Protection (Access Modification) (Health) Regulations 1989
- Data Protection Act 1988 (Section 16(1)) Regulations 2007



# Prospective Legislative Regime

---

- General Data Protection Regulation – replaces existing law in May 2018
- Irish Data Protection Bill



# General Data Protection Regulation

---

- Retains existing data protection concepts and requirements
- Increases obligations on controllers/processors and affords new rights to data subjects



# Key Data Protection Terminology

---

- Definitions (Article 4) - Similar to existing regime
- **Personal data** – relates to identified or identifiable living individuals (not anonymised data)
- **Processing** – widely defined – includes any collection, recording, organisation structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, erasure or destruction of data
- **Controller** – entity which determines the purposes and means of processing of personal data
- **Processor** – entity which processes personal data on behalf of controller – e.g. outsource service provide



# Examples of Personal Data

---

- Personnel/employment files
- Customer correspondence (email and hard copy)
- Application forms
- Financial information
- Records of telephone calls
- E-mails
- Records of websites visited
- CCTV images



# Insurance companies – Data Protection

---

- Why is data protection important to insurance companies?
- Holder of large repository of customer data (held by or on behalf of insurers)
- Focus by DPC on insurance companies' activities – including use of Private Investigators



# Main Controller Obligations





# Fair And Transparent Processing

---

- Articles 5(1)(a), 13 and 14
- Data Subject must be made aware:
  - Controller holds personal information about him/her
  - Purposes for which information kept
  - Disclosures of data
  - Certain other details (additional to those required under existing law)



# Making Processing Legitimate

---

- Duty to legitimise processing (Article 6)
- Justify on one of the following grounds:
  - consent of data subject
  - processing necessary for performance of contract (to which data subject party)
  - legal obligation (non-contractual)
  - legitimate interests



# Special Categories of Personal Data

---

- Personal data relating to:
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade union membership
  - physical or mental health
  - sex life or sexual orientation
  - genetic data
  - biometric data for identification



# Special Categories of Data *cont'd*

---

- Controller must satisfy one of the following grounds (Article 9):
  - explicit consent of data subject
  - exercise/performance of employment rights/obligations
  - obtaining legal advice/legal proceedings or the establishment, exercise or defence of legal claims
  - processing necessary for reasons of substantial public interest on the basis of Union or member state law



# Other Main Data Protection Obligations

---

- ***Purpose Limitation (Article 5(1)(b)):*** Data to be kept for Specified, Explicit and Lawful Purposes and not further processed for any incompatible purposes
- ***Data Minimisation (Article 5(1)(c)):*** Data should be adequate, relevant and not excessive
  - Keep only the minimum amount of personal data needed for the purpose for which it is being processed
  - Avoid keeping irrelevant or excessive data
- **Obligation to keep personal data accurate and up-to-date (Article 5(1)(d))**



# Data Security (Article 32)

---

- Appropriate security measures must be taken against unauthorised access to, alteration, disclosure or destruction of personal data
  - state of the art and cost of implementing security measures
  - severity for rights and freedoms of data subjects that might result from unauthorised disclosure
- Potential measures – pseudonymisation, encryption, ability to ensure confidentiality of systems, ability to restore availability and access to personal data, regular testing of security measures



# Security Breach Notifications (Article 33/34)

---

- Data Security Breach Notification
  - Mandatory notifications to Data Protection Commissioner within 72 hours – unless breach unlikely to result in a risk to data subjects
  - Mandatory notification to affected data subjects “without undue delay” – where there is a high risk to data subjects
  - Data processors required to notify data controllers of data security issue without undue delay



# Record Retention - Deletion

---

- Obligation not to keep personal data for any longer than is necessary
- Data should not be kept on a just-in-case basis
- Record Retention Policy





# Transfers Abroad (Chapter V)

---

- Prohibition on Transfer of Personal Data outside European Economic Area (EU, Iceland, Norway and Liechtenstein) unless recipient country ensures adequate protection
- Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay found to have adequate protection.



# Transfers Abroad cont'd

---

- Prohibition will not apply, amongst other things, if:
  - data subject consent
  - transfer necessary for purpose of obtaining legal advice or for legal proceedings
  - data transfer agreement, in the form approved by the European Commission
  - Binding corporate rules
  - Privacy shield (if transfer is to United States)



# Access Rights (Article 15)

---

- Rights of data subjects to a copy their personal data
- Similar rights to existing law, but:
  - no charge
  - 30 day period (can be extended by up to 2 further months)
  - no exemptions enshrined in GDPR – must be reflected in local law (Data Protection Bill or regulations made under it)



# GDPR – “One Stop Shop”

---

- “One Stop Shop” - Single EU Regulator
  - Organisations operating in multiple jurisdictions will be regulated primarily by national data protection authority in the country of organisation’s “main establishment”
  - One Stop Shop now somewhat “watered down” – includes consultation obligations with other relevant authorities



# GDPR – Right to be forgotten

---

- Right to erasure (“right to be forgotten”)
  - strengthening of pre-existing rights of data subjects to require erasure of personal data
  - particular emphasis on the right of a data subject to require erasure of data made available when he was still a child



# GDPR – Data Portability

---

- Right to Data Portability (Article 20)
  - Right to receive data which (s)he provided to data controller in a structured, commonly used and machine readable format and to have it transmitted to another data controller where:
    - processing is based on consent or contract with the data subject; and
    - processing is carried out by automated means
  - Consider strategy for collection and use of personal data
- Article 29 WP Guidance – data “provided” to controller includes data which controller “observed” about data subject – e.g. includes data analytics?



# GDPR – Internal Governance/Responsibility

---

- Increased internal governance and responsibility
  - removal of registration obligation (Insurance Companies will no longer need to register)
  - requirement replaced with obligation to adopt internal policies and procedures which demonstrate compliance with data protection laws
  - privacy by default and design
  - Data Protection impact assessments



# GDPR – Internal Governance/Responsibility

---

- Various entities will be required to appoint a data protection officer (“DPO”) to oversee compliance with the Regulation:
  - all public authorities (except courts)
  - bodies which are likely to be monitoring data subjects on a large scale
  - controllers or processors with large scale of special categories of data
  - other categories to the extent required by Member State law
- Likely that Insurance Companies will be required to have DPO





# Data Protection Officer

---

- DPO – to be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil DPO tasks
- DPO may be employee or third party service provider
- Need to ensure that DPO is involved properly and in a timely manner in all issues relating to protection of personal data
- DPO cannot be dismissed or penalised for performing DPO tasks



# Tasks of Data Protection Officer

---

- Inform and advise on data protection
- Monitor compliance with GDPR and policies and procedures
- Advice on data protection impact assessments



# GDPR – Fines

---

- New: Severe financial penalties
  - potential fines up to 4% of annual worldwide turnover or €20 million (whichever is greater)
  - fines may be levied by Data Protection Authorities themselves



# GDPR – Further legislative measures

---

- Further local legislative measures required in specified circumstances, e.g.:
  - further local legislative measures required to reflect (i) exemptions from obligations and (ii) exemptions from access rights – provided that the local measures comply with the general parameters set out in GDPR
  - further categories of organisations required to have DPOs
  - establishment of Data Protection Authority
- General Scheme of Data Protection Bill published on 12 May 2017



# GDPR – Main Implications for Insurers

---

- **Data Inventory** – *what, where, why and for how long* – need to carry out full inventory of personal data
- **Data protection notices and various data protection policies and procedures** – review of existing policies and procedures and potential need for additional policies
- **Controller/processor agreements** – will require more detail
- **Privacy statements** – will require more detail
- **Data protection audits/assessments; Data Protection Impact Assessments** – new forms of processing are likely to require data protection impact assessments
- **Data security breaches** – mandatory reporting



# GDPR – Main Implications for Insurers

---

- **DPO Appointment** – Requirement to ensure that DPO is appointed and that there is appropriate support – Potential need to enshrine guaranteed independence in role
- Potential Fines “Ups Ante” in respect of compliance



# GDPR – Compliance Steps

---

- Time to “spring clean privacy practices” and prepare for GDPR
  1. Get senior “buy in” to DP compliance – without senior buy in, compliance will be hard to achieve
  2. Data Inventory – Review/health check of data and processing activities – data protection audit/assessment
  3. Review basis for processing – e.g. consent, legitimate interests, necessary for contract performance etc
  4. Policies, procedures and notices – review/develop necessary internal policies/procedures and notices



# GDPR – Compliance Steps

---

5. DPO appointment
6. Review third party processing and international transfers
7. Keep an eye out for prospective data protection bill and DPC guidance

Main message: No need to panic, but if an organisation hasn't started, start now