ORIC INTERNATIONAL

The Scenario Universe

7 July 2015

Caroline Coombe

Today's agenda

- Introduction to ORIC
- The Scenario Universe Overview
- The Process
- Internal Data Sources
- External Data Sources – Data, Scenarios, Key Risk Indicators
- Community

About ORIC

ORIC International's core aim is:

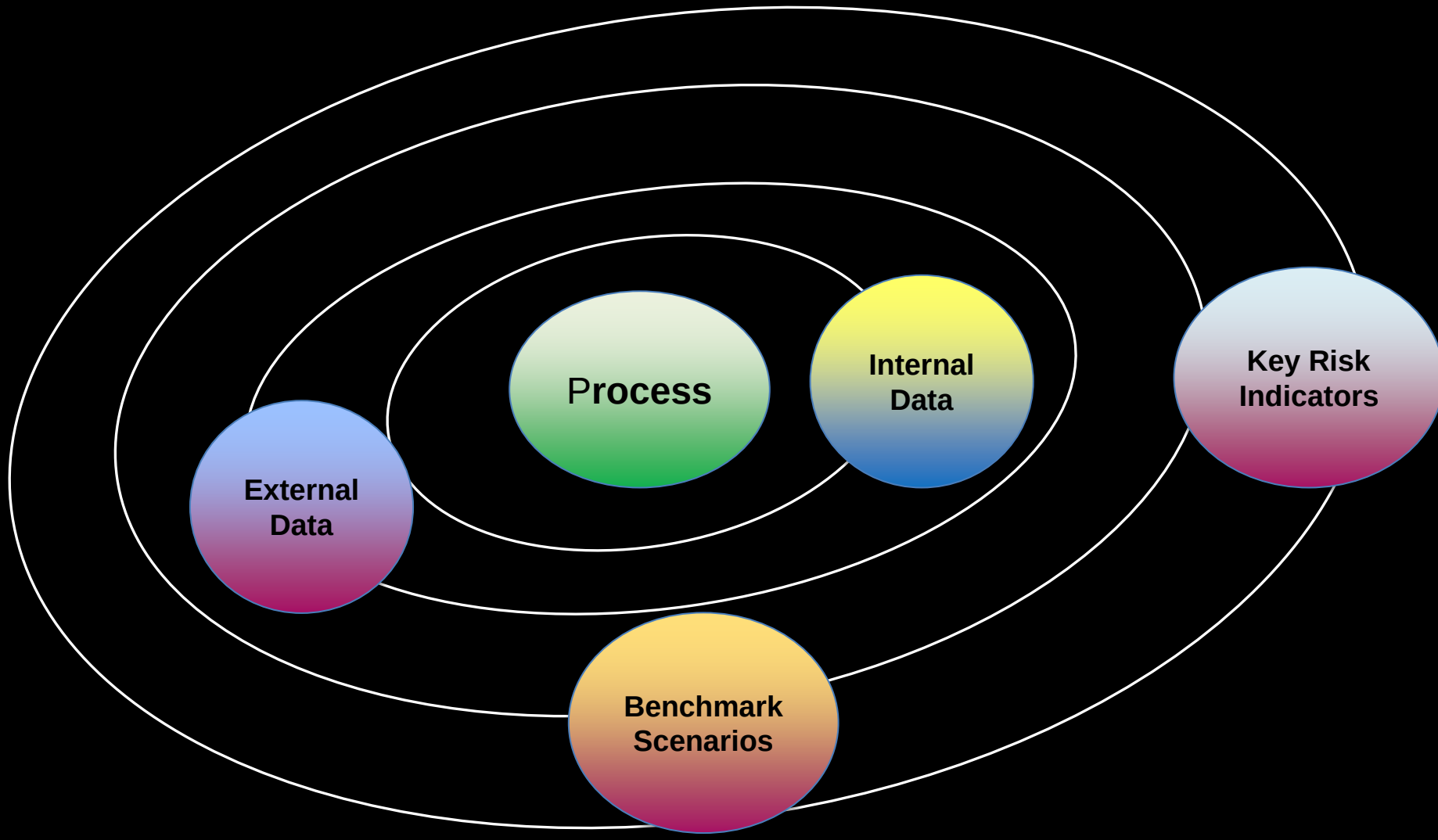
"To advance operational risk management and measurement"

<u>ORIC International Scenario Expertise</u>

- Scenario analysis working group
  - Made up of 10-12 industry experts from our member firms
  - Aim of the group is to develop resources for the ORIC member base through sharing knowledge and best practice
  - Working has conducted member base wide studies into Scenario Analysis approaches, correlations and Scenario Assessment benchmarking.

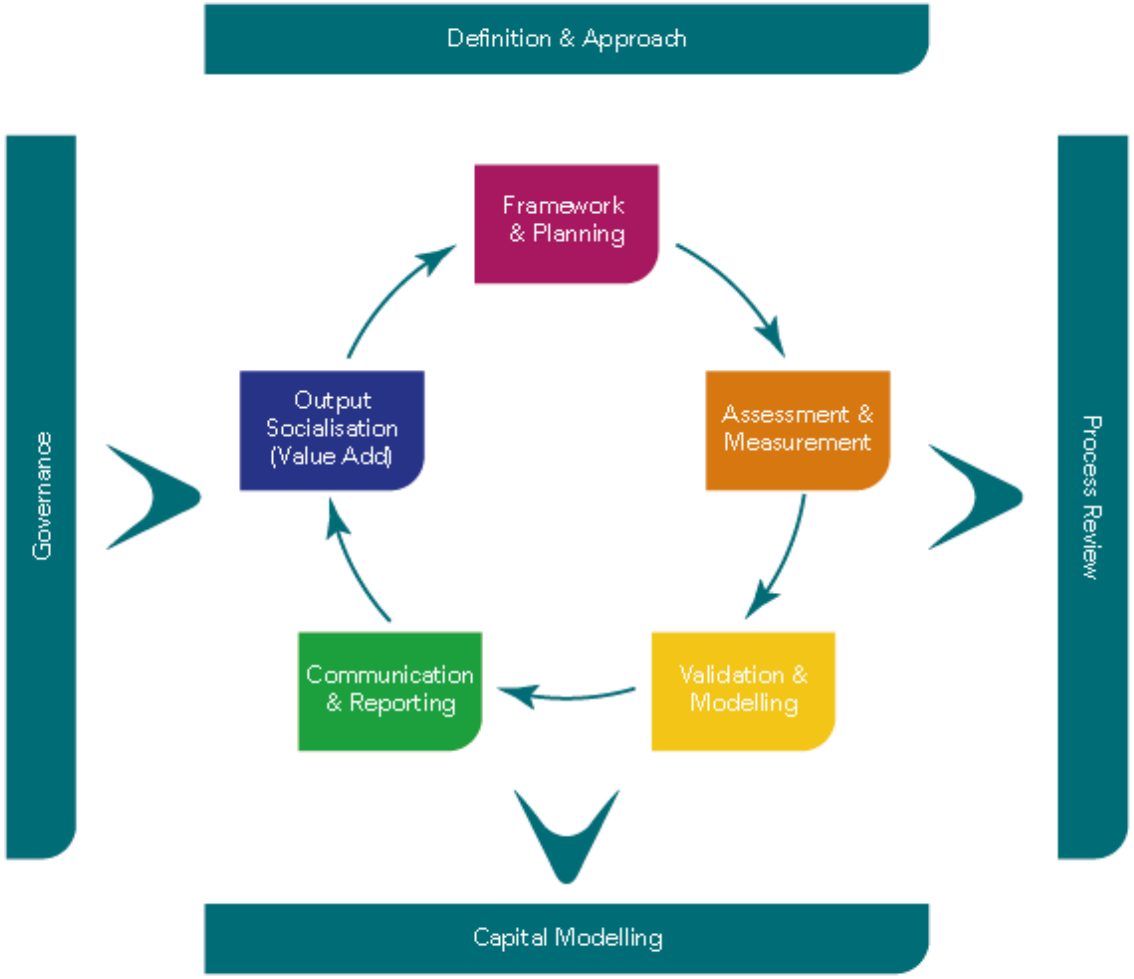
- First issued best practice in 2010 and 2015 has seen the launch of our latest best practice guidance

The Scenario Universe Concept



The Scenario Analysis Process

The Process Cycle



The Process Cycle

Definition & Approach

- Common characteristics:
  - Extreme
  - Plausible
  - Manifestation of risk
  - Material-impact
  - Forward Looking
  - Hypothetical situations
  - High severity/low frequency
  - 1/200/ 99.5% confidence level
  - ‘What if’ analysis
  - Event simulation

Main approach considerations:

- Process drivers such as risk capital allocation, regulatory requirements or effective operational risk management and measurement

- Who are the stakeholders within the process? Risk management/professionals, senior management/Board, shareholders

The Process Cycle

Capital Modelling

- Scenario analysis can provide frequency and severity data points required for certain types of frequency and severity models (statistical distributions)
- Especially for tail events for which there is no/limited internal historical risk event data
- Need to take particular take to avoid double counting boundary risks
- Ensure that no material risks are missed

The Process Cycle

Process Review

- The majority of firms run scenario analysis as an annual process

- It is important to build in time in the process cycle to review the following:
  - the performance of the process;
  - relevance and use of the outputs; and
  - necessary enhancements that could improve the process.

- It is important and useful to be able to benchmark a firms internal approach to that used in peer firms. This can be done by participating in industry forum or through a consortium studies such as those conducted by ORIC International.

The Process Cycle

Governance

- Scenario analysis form an integral part of the op risk management culture
- The results of this process should have a meaningful impact of the firms governance and the governance structure should support the process from policy approval to output validation.
- The four main governance pillars involved in scenario analysis are:
  - The Board
  - Risk Committee/Executive committee
  - Risk function
  - Business units
- It is important to consider how to engage senior management and the role of Internal Audit in the process.

Framework and Planning

Framework development:

- Scenario analysis is an important part of an ERM framework
- Firms should have a clear policy that sets our the firms approach
- The policy should also define the scope of the scenario analysis process
- Ensure that the framework is appropriately documented

Planning stage:

- Scenario identification
- Gathering supporting information
- Considering the number of scenarios to run
- Workshop planning including
  - Workshop attendee considerations such as bias, personality clashes
  - Materials required

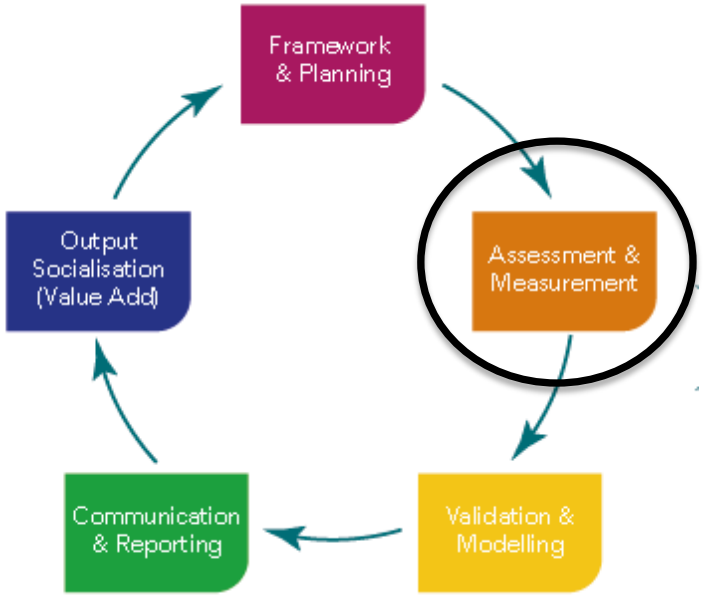
Assessment & Measurement

- Expert judgements made in workshop environment

- Severity assessments
  - Direct impacts
  - Indirect impacts

- Frequency assessments
  - Most common assessment points: 1 in 10 yrs, 1 in 20 yrs
  - Range from 1 in 1 yr to 1 in 200 yrs

- Recording discussions
  - Detail and document material processes, key elements of the scenario assessment including:
    - Storyline, inputs, outcome of expert assessment, rationale for the assessment, mitigation strategies, any additional information.



Validation & Modelling

Validation:

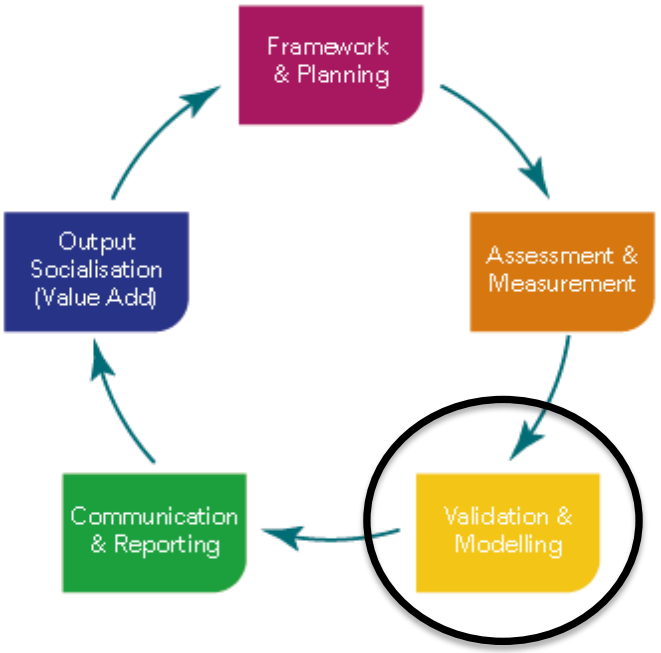
- Workshop outputs should be reviewed for clarity, ambiguity and consistency.

- Dealing with bias – understanding and controlling biases

Modelling:

- A firm must consider if there is a need to aggregate scenarios at a certain level and if so, how they will do this.

- Also must consider if there is a need to correlate the scenario outputs with the capital charges for other risk categories.



Communication & Reporting

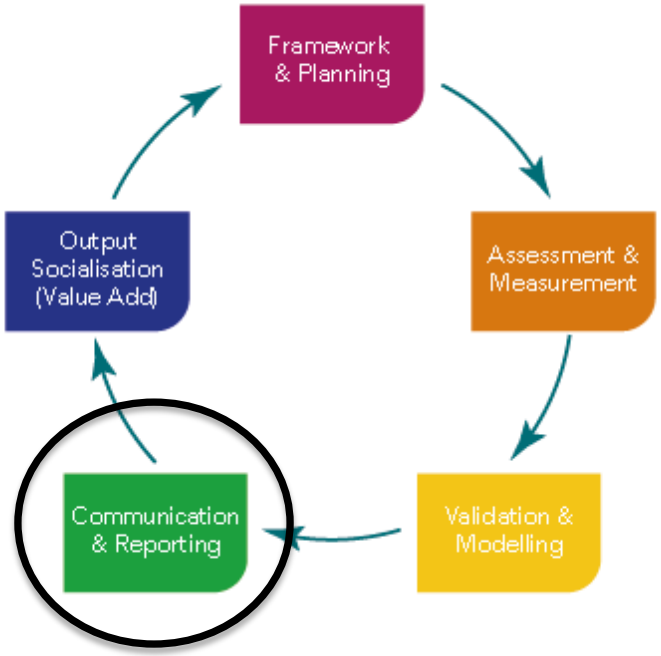
Recent ORIC survey found that 84% sign off the scenario analysis results at a Group Risk Management level

Sign off will depend on the firms governance process

Those involved in reporting must understand how the outputs were derived and their usage

As a minimum the following functions should receive the outputs: Board; Executive Committee; Risk committees and Group Actuarial

Must consider how to engage senior management in the reporting of the results



Output Socialisation

A firm must identify all business units and functions that have an interest in the scenario analysis results

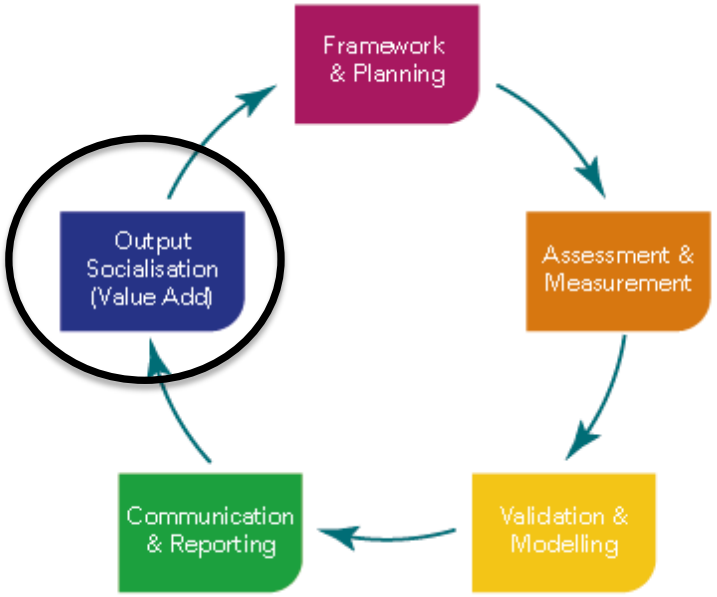
As a minimum results should be shared with:

- Senior Management, the Board and relevant committees

- Actuarial function

- Audit/Independent assurance functions

- Relevant Heads of Department



Process Maturity

	Framework Development
Developing	Scenario definition is not or loosely defined Methodology is not documented/ Partially documented Objectives of the process are not clear but decided on an ad hoc basis The analysis results are not used in any tangible way in the business
Peer Equal	Scenario definition is defined Fully documented Objectives of the process are clear The results are used occasionally
Advanced	Definition is clearly defined and reviewed at least annually for appropriateness Definition and process are fully documented and regularly reviewed for appropriateness Objectives of the process are clearly defined, full documented and understood by all those involved in the process

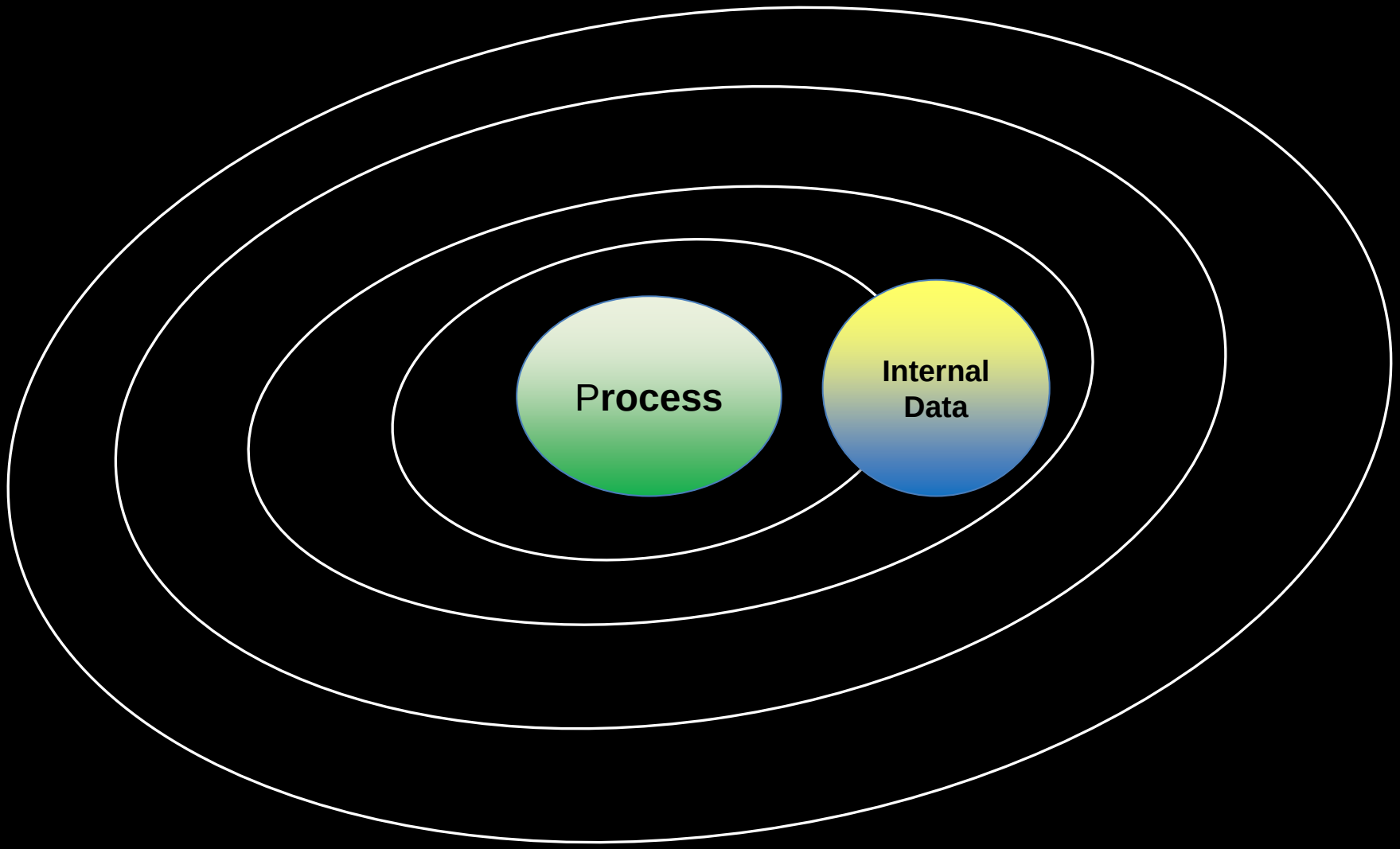
Full diagnostic contains benchmarks for all 6 key process features.

Identifies 3 levels of maturity from developing to advanced.

Enables benchmarking of current approaches.

Provides indications of process improvements required to move towards more advanced scenario analysis process maturity

The Scenario Universe Concept



Internal Data Inputs

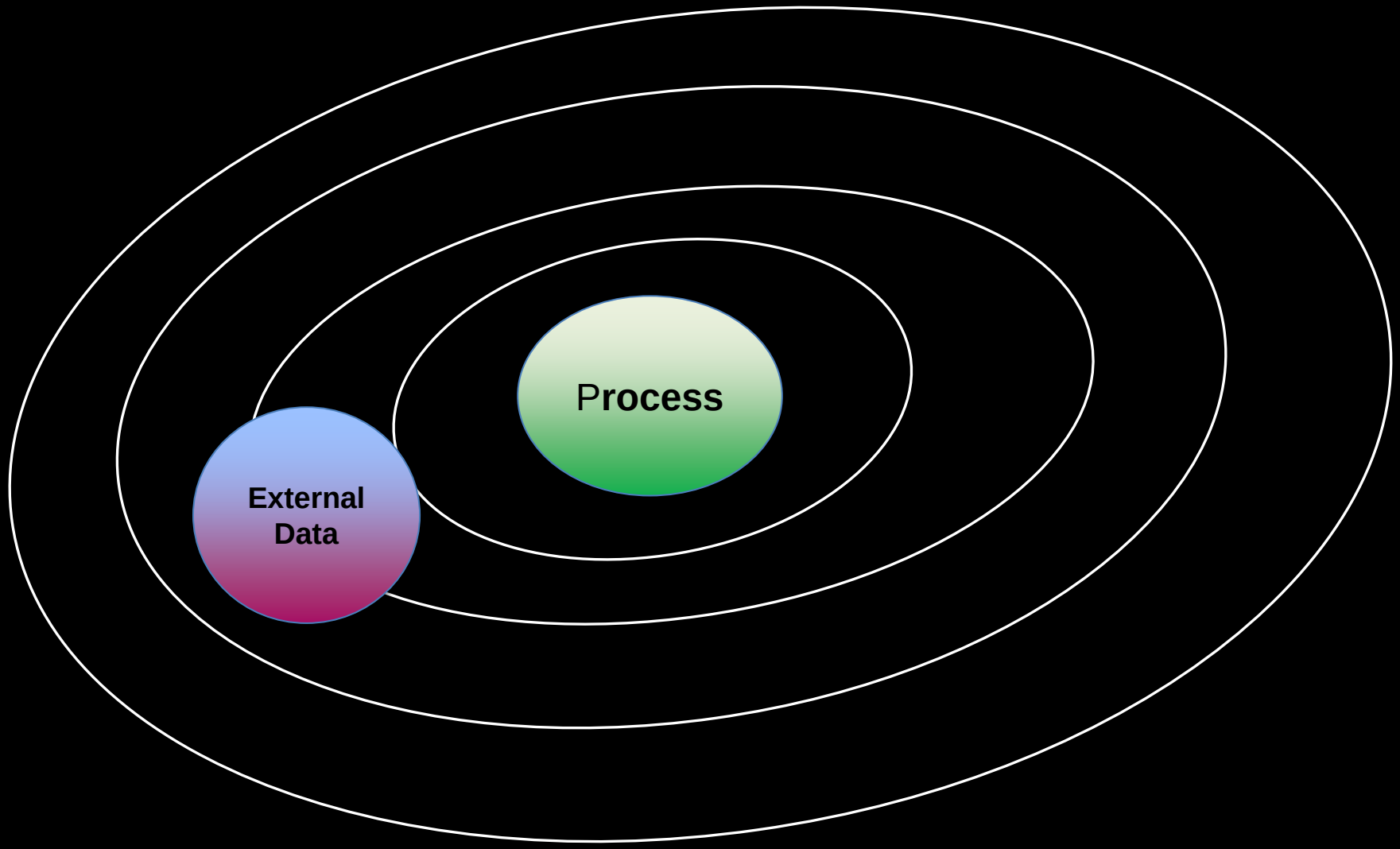
Internal Resources Available

Source	Description	Pros	Cons	Market use
Expert Judgement	The thoughts, knowledge and experience of subject matter experts in their field	➢ Internally available ➢ No additional cost ➢ Readily available	➢ Subjective and prone to bias ➢ Limited to a firms/ an individuals experiences ➢ Limited validation techniques available ➢ Normally harvested through time-consuming workshops	Firms are making extensive use of subject matter expert judgment for scenario assessments, scenario validation and setting scenario correlations.
Risk and Control Self-Assessment Outputs (RCSAs)	The outputs of a risk assessment regime commonly in place within an ERM framework	➢ Internally available ➢ No additional cost ➢ Readily available	➢ Subjective and prone to bias ➢ Limited to a firms/ an individuals experiences ➢ Only considers risks that are known to the firm	Widely used as a desktop exercise within risk management
Internal Risk Event Loss Data	The data captured internally regarding risk events that have occurred within the firm	➢ Internally available ➢ Readily available ➢ Key insights for likelihood and severity assessments	➢ Dependent on having an effective risk event capture process in place ➢ Limited to a firms/ an individuals experiences ➢ Some interpretation required	Widely used where a process is in place
Internal Key Risk Indicators	Data resulting from key risk indicator vs risk appetite monitoring and reporting	➢ Can provide insights into evolving risks ➢ Indicate risks that are outside appetite	➢ Reliant on having the correct indicators in place and a strong KRI review and reporting process	Not widely used but becoming more popular

Main challenges of using internal resources/data:

- Data scarcity
- Subjectivity
- Limited to firm/expert experience
- Limited challenge and validation available

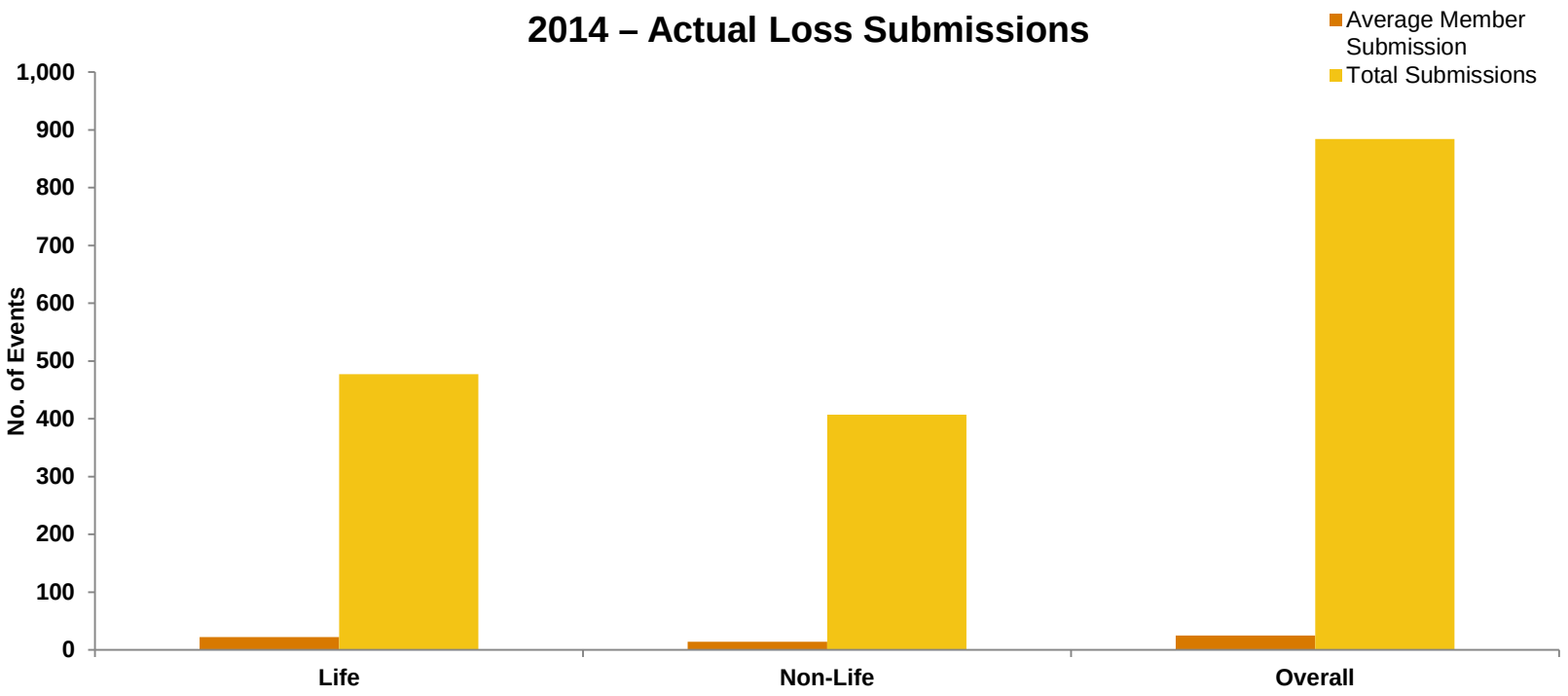
The Scenario Universe Concept



External Data Inputs

Consortium Data

- Consists of nearly 7,500 risk events, with a combined value of £3.49bn
- Includes both Actual Losses and Near Misses
- Both Qualitative and Quantitative information supplied



Public Risk Event Data

- Over 17,000 risk events collected from the public domain
- Approximately 1,100+ of these are Insurance-specific newsflashes

Services Settings Operational Risk Consortium Limited

Home ▸ Newsflashes ▸ **Newsflashes**

View Download Selected | Add To Your Favourites Remove From Your Favourites

Search: Search Clear Advanced Filter Clear Filter

Filter on: (No Filter) Date: (No Filter)

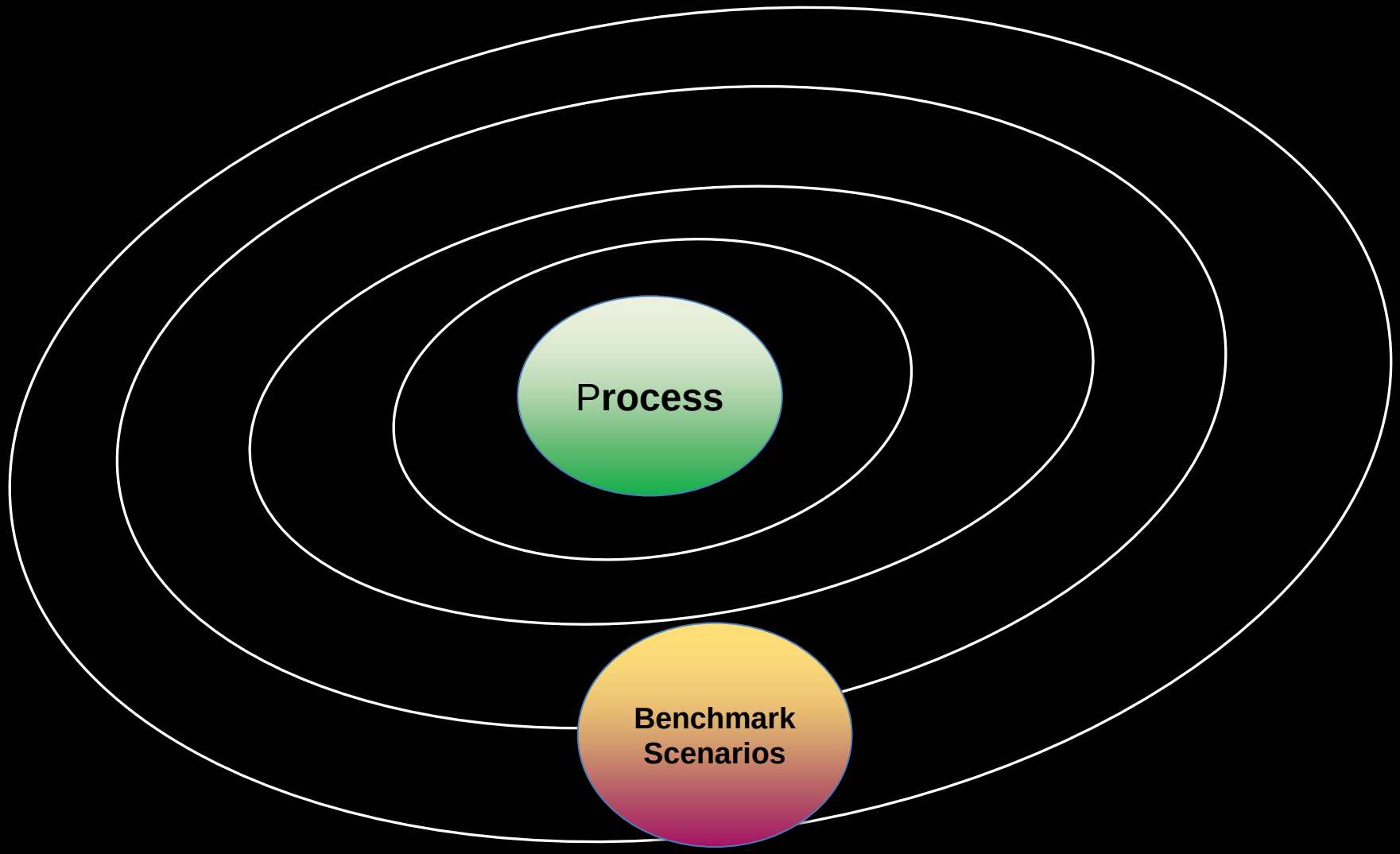
Page: 1 Names [All] # A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Total: 1167 Page 1 of 24

Date [1]	Title	Amount	Names [2]	Business Line
09/03/2015	Insurer RSA likely to face maximum fine of about €5m	5,000,000.00 EUR	RSA Insurance Group (Royal and Sun Alliance)	Corporate Services
08/03/2015	National Insurance employee arrested for bribery and fraud		Bituah Leumi	Corporate Services
05/03/2015	Aetna sold policies without approval from NC Department of Insurance	0.00 USD	Aetna Inc.; North Carolina Department of Insurance	Life Assurance
05/03/2015	7 insurance companies fined for negligence in alleged fraud case	11,400,000.00 TWD	Shin Kong Life; Cathay Century Insurance; CTBC Life; Taian Insurance / 泰安產物保險公司; BankTaiwan Life Insurance; Chung Kuo Insurance / 兆豐保險; TransGlobe Life Insurance; Financial Supervisory Commission (FSC) / 行政院金融監督管理委員會	Life Assurance
27/02/2015	NAICOM fines insurance firms N543.69m	543,690,000.00 NGN	National Insurance Commission (NAICOM)	Market Supervision
27/02/2015	State Farm to pay $352.5m to settle Texas residential overcharge case	352,500,000.00 USD	State Farm Lloyd's; Texas Department of Insurance	General Insurance
25/02/2015	Anthem hack: Millions of non-anthem customers could be victims		Anthem Inc. (previously WellPoint Inc.)	Life Assurance
24/02/2015	FCA fines Aviva Investors £17.6m for systems and controls failings that led to its failure to manage conflicts of interest fairly	17,607,000.00 GBP	Aviva	Investment Management
16/02/2015	RSA Ireland probe at 'advanced stage,' Irish Central Bank says		RSA Insurance Group (Royal and Sun Alliance); Central Bank of Ireland / Banc Ceannais na hEireann	Corporate Services
13/02/2015	Insurer hit with $4.5m class action bad faith verdict in Nevada	4,500,000.00 USD	Everest Indemnity Insurance Company	General Insurance
05/02/2015	Health insurer Anthem hit with cyber attack		Anthem Inc. (previously WellPoint Inc.)	Life Assurance
03/02/2015	Former California agent pleads guilty in $6m fraud case	5,900,000.00 USD	Hamilton Brewart Insurance Agency; Universal Bank	Insurance Broking
03/02/2015	Insurance agent ran $10m Ponzi scheme	10,000,000.00 USD	ISC Inc	Insurance Broking
12/01/2015	Mercury in California ordered to pay $27.5m for unapproved broker fees	27,500,000.00 USD	Mercury Insurance; California Department of Insurance	General Insurance
07/01/2015	Missouri fines insurer nearly $162k for misstatements to policyholders	161,800.00 USD	Humana; Missouri Department of Insurance	Life Assurance
23/12/2014	Man who tried to commit insurance fraud gets suspended sentence		Citadel Insurance	General Insurance
22/12/2014	Insurer Delta Lloyd fined, told to dismiss CFO by central bank	22,800,000.00 EUR	Delta Lloyd; De Nederlandsche Bank	Corporate Services

Uses within the scenario analysis process

- Scenario generation
  - Use consortium and public risk events to find large losses that your peers have suffered
- Inform scenario assessments
  - Provide workshop participants with valuable contextual market information
  - Can provide useful severity assessment information – how much have large losses cost peer firms historically
- Inform the validation of scenario assessments
  - Challenge assessment given by benchmarking the assessment against similar historical large losses

The Scenario Universe Concept



Benchmark Scenarios

- ORIC International have developed a set of 38 benchmark scenarios complete with technical specifications.
- Developed by the industry experts through the ORIC International Scenario Analysis Working Group
- Considered by the Working Group to be a complete set of scenarios that an Insurance firm would want to consider that enable firms to validate the completeness of their internal scenario set
- Relevant public risk events, consortium risk events, key risk indicators and library scenarios have been mapped to each benchmark scenario that provide useful contextual information that can assist in the assessment of scenarios

Scenario Specification

General

Name	Cyber-attack for the purposes of fraudulent activity		
Description	A party attacks the firm's computer systems with the purpose of defrauding the firm or the theft of data. Excludes: Cyber-attacks for the purpose of business disruption i.e. viruses. Includes: Hacking		
AML specific	Yes	Generate reputational consequences	No
KYC specific	No	Business resilience specific	Yes
SoX specific	No	Information security specific	Yes
Conduct specific	No	Litigation specific	No
Boundary specific	No		

Root Causes

Name	Poor IT security
Causal type	Systems (IT) / Poor IT Security
Description	Poor or inadequate IT security controls to prevent a cyber-attack for example out of date/inadequate firewall protection

Control Types

Names	Information and Infrastructure Controls
	Systems Access Right Reviews
	System Activity Logs

Direct Impacts

Name	External litigation fees and costs
Impact type	External litigation fees and costs
Description	External litigation fees and costs of litigating against external parties who have committed fraud through the use of cyber attacks

Indirect Impacts

Name	Negative effect on a firm’s reputation as a result of having inadequate controls to prevent cyber attacks
Impact type	Reputational Impacts
Description	A measure of the reputational impact on the organisation, which may be measured through adverse media coverage, loss of client and customer business, deterioration in share price or changes in market perception, as determined through opinion polls.

Cont…

Example Public Newsflash			
Title	Health insurer Anthem hit with cyber attack		
Event date	05/02/2015	Source	Insurance Journal (www.insurancejournal.com)
Country	United States of America	Amount	Undisclosed
Involved	Anthem Inc. (previously WellPoint Inc.)		

Example Key Risk Indicator	
Name	E-Crime and System Security - Number of Losses Due to Hacking and Disruption
Description	The total number of losses to the organisation from information technology security violations, unauthorised logins, hackers sniffing web sessions, TCP/IP hacking and other forms of service denial attempts, during the preceding 12 calendar months.
Measurement Frequency	Daily
Reporting frequency	Daily
Frequency of expected change	Ongoing
Measurement rules	Include all losses due to information security hacking and service denial during the preceding 12 months, whether from unauthorised logins, hackers sniffing web sessions, TCP/IP hacking or other means. Exclude information technology security issues caused by employees and contractors.
Calculation method	Count the number of losses meeting measurement criteria.

Linked Scenario Storyline	
Name	Electronic communication interception

Risk Categories	
Primary risk category	External Fraud / Systems Security
Secondary risk categories	External Fraud
	Theft and Fraud
	Theft of assets
	Forgery, impersonation

Business Functions	
Primary business function	IT
Secondary business functions	Claims
	Customer Service/Policy Administration
	Sales and Distribution
	Underwriting

Properties	
Tags	Cybercrime; Identity Theft; Insurance Fraud

Scenario Universe (2015)

- Detailed and informative best practice guide that covers all aspects of the scenario analysis process
- All 38 benchmark scenario specifications

EVENT OFFER!!!!

Order a copy today and save **£200**!

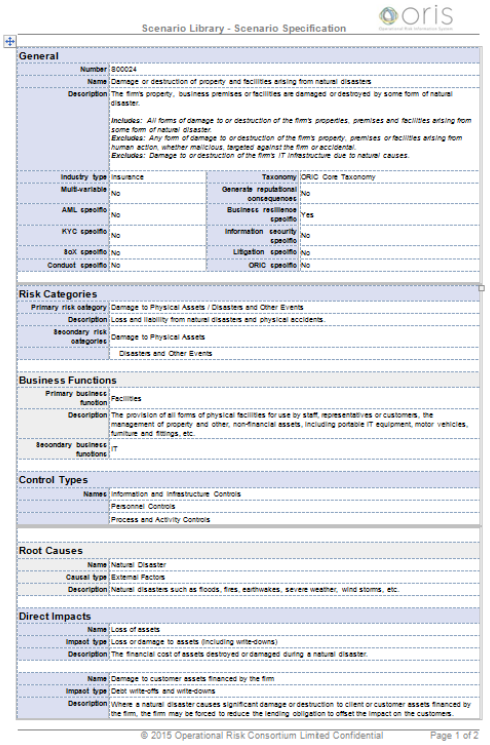
Todays price for IOR Scenario event attendees:

£550!!!

Normal price: £750

Scenario Library

- Repository of over 180 scenario storylines with detailed technical specifications
- Each of these have been mapped to relevant consortium losses, newsflashes and KRIs.
- Relevant scenarios have been mapped to 38 overarching benchmark scenarios
- The database can be filtered on operational risk category, business function, meta data tags and many other fields
- Each specification can be downloaded in PDF, word or printed



Scenario Library - Scenario Specification

General

Number	800024
Name	Damage or destruction of property and facilities arising from natural disasters
Description	The firm's property, business premises or facilities are damaged or destroyed by some form of natural disaster. *Includes: All forms of damage to or destruction of the firm's properties, premises and facilities arising from some form of natural disaster.* *Excludes: Any form of damage to or destruction of the firm's property, premises or facilities arising from human action, whether malicious, targeted against the firm or accidental.* *Excludes: Damage to or destruction of the firm's IT infrastructure due to natural causes.*

Industry type	Insurance	Taxonomy	ORIC Core Taxonomy
Multi-variable	No	Generate reputational consequences	No
AML specific	No	Business resilience specific	Yes
KYC specific	No	Information security specific	No
SoX specific	No	Litigation specific	No
Conduct specific	No	ORIC specific	No

Risk Categories

Primary risk category	Damage to Physical Assets / Disasters and Other Events
Description	Loss and liability from natural disasters and physical accidents.
Secondary risk categories	Damage to Physical Assets
	Disasters and Other Events

Business Functions

Primary business function	Facilities
Description	The provision of all forms of physical facilities for use by staff, representatives or customers, the management of property, and other, non-financial assets, including portable IT equipment, motor vehicles, furniture and fittings, etc.
Secondary business functions	IT

Control Types

Names	Information and Infrastructure Controls
	Personnel Controls
	Process and Activity Controls

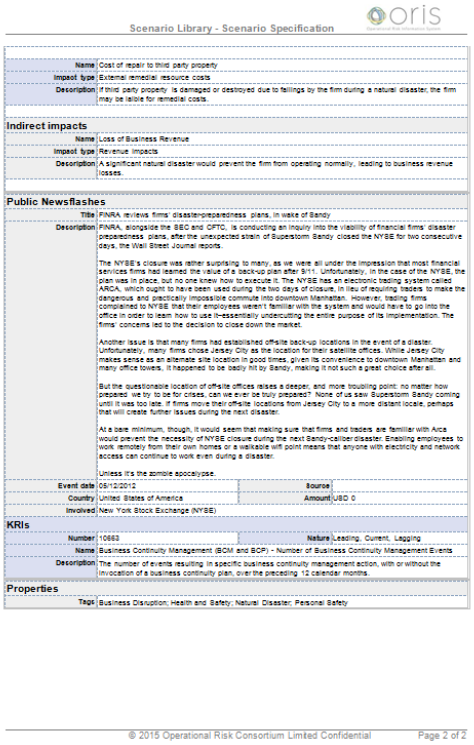
Root Causes

Name	Natural Disaster
Causal type	External Factors
Description	Natural disasters such as floods, fires, earthwakes, severe weather, wind storms, etc.

Direct Impacts

Name	Loss of assets
Impact type	Loss or damage to assets (including write-downs)
Description	The financial cost of assets destroyed or damaged during a natural disaster.
Name	Damage to customer assets financed by the firm
Impact type	Credit write-offs and write-downs
Description	Where a natural disaster causes significant damage or destruction to client or customer assets financed by the firm, the firm may be forced to reduce the lending obligation to offset the impact on the customers.

© 2015 Operational Risk Consortium Limited Confidential Page 1 of 2



Scenario Library - Scenario Specification

Name	Cost of repair to third party property
Impact type	External remedial resource costs
Description	If third party property is damaged or destroyed due to failings by the firm during a natural disaster, the firm may be liable for remedial costs.

Indirect impacts

Name	Loss of Business Revenue
Impact type	Revenue impacts
Description	A significant natural disaster would prevent the firm from operating normally, leading to business revenue losses.

Public Newsflashes

Title	FINRA reviews firms' disaster-preparedness plans, in wake of Sandy		
Description	FINRA, alongside the SEC and CFTC, is conducting an inquiry into the viability of financial firms' disaster preparedness plans, after the unexpected strain of Superstorm Sandy closed the NYSE for two consecutive days, the Wall Street Journal reports. The NYSE's closure was rather surprising to many, as we were all under the impression that most financial services firms had learned the value of a back-up plan after 9/11. Unfortunately, in the case of the NYSE, the plan was in place, but no one knew how to execute it. The NYSE has an electronic trading system called ARCA, which ought to have been used during the two days of closure, in lieu of requiring traders to make the dangerous and practically impossible commute into downtown Manhattan. However, trading firms complained to NYSE that their employees weren't familiar with the system and would have to go into the office in order to learn how to use it—essentially undercutting the entire purpose of its implementation. The firms' concerns led to the decision to close down the market. Another issue is that many firms had established offsite back-up locations in the event of a disaster. Unfortunately, many firms chose Jersey City as the location for their satellite offices. While Jersey City makes sense as an alternate site location in good times, given its convenience to downtown Manhattan and many office towers, it happened to be badly hit by Sandy, making it not such a great choice after all. But the questionable location of offsite offices raises a deeper, and more troubling point: no matter how prepared we try to be for crises, can we ever be truly prepared? None of us saw Superstorm Sandy coming until it was too late. If firms move their offsite locations from Jersey City to a more distant locale, perhaps that will create further issues during the next disaster. At a bare minimum, though, it would seem that making sure that firms and traders are familiar with Arca would prevent the necessity of NYSE closure during the next Sandy-caliber disaster. Enabling employees to work remotely from their own homes or a walkable wifi point means that anyone with electricity and network access can continue to work even during a disaster. Unless it's the zombie apocalypse.		
Event date	05/12/2012	Source	
Country	United States of America	Amount	USD 0
Involved	New York Stock Exchange (NYSE)		

KRIs

Number	10663	Nature	Leading, Current, Lagging
Name	Business Continuity Management (BCM and BCP) - Number of Business Continuity Management Events		
Description	The number of events resulting in specific business continuity management action, with or without the invocation of a business continuity plan, over the preceding 12 calendar months.		

Properties

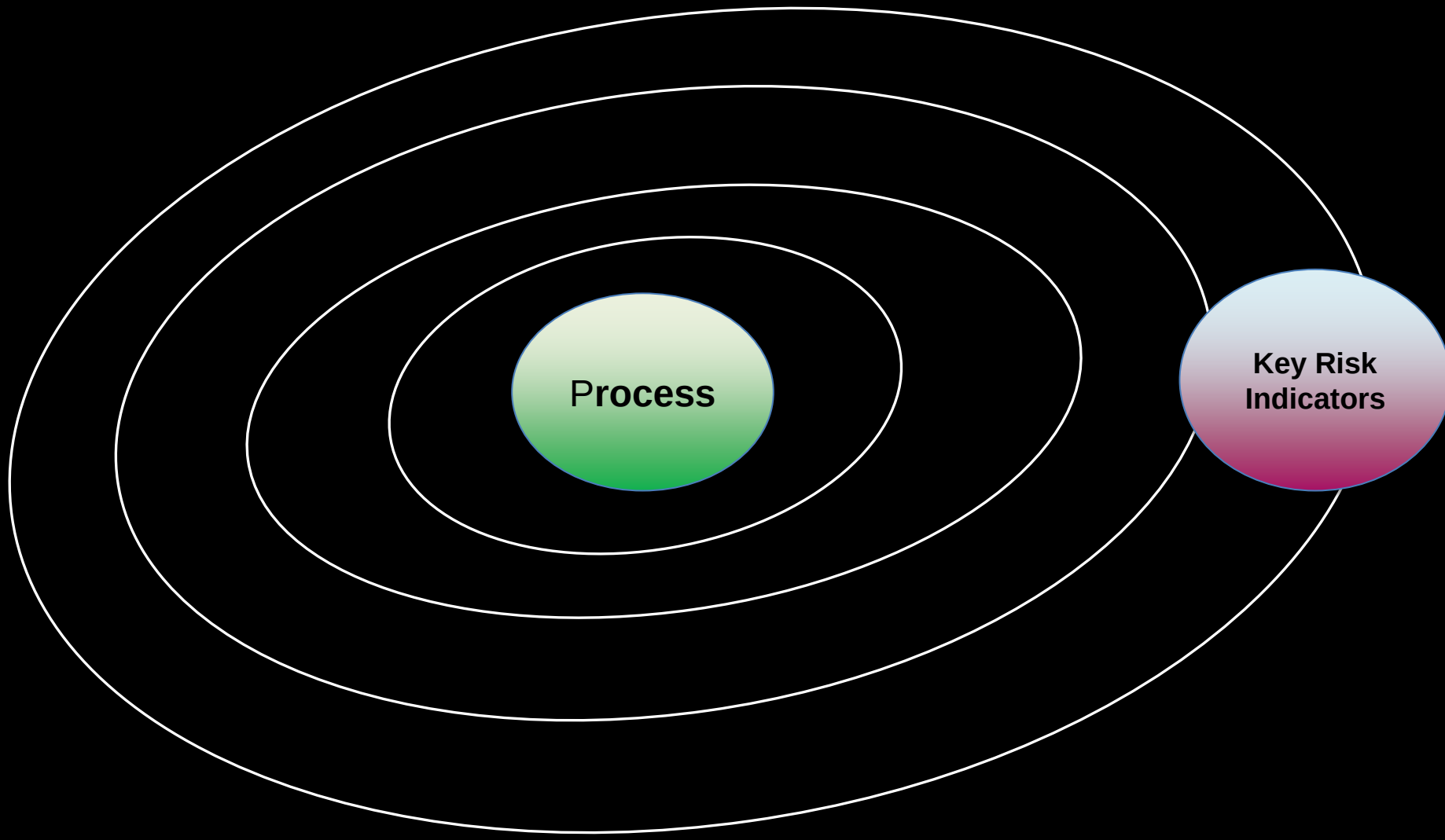
Tags	Business Disruption, Health and Safety, Natural Disaster, Personal Safety

© 2015 Operational Risk Consortium Limited Confidential Page 2 of 2

Uses of Benchmark Scenarios

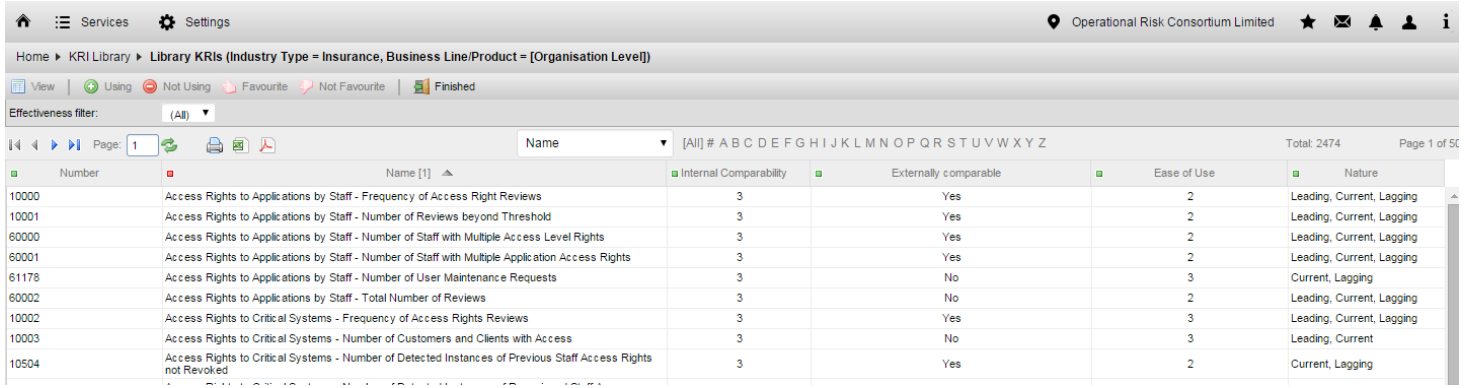
- Challenge the completeness of the existing scenario set
- Scenario generation inputs
- Workshop prep materials – what should workshop participants be thinking about in the lead up to a workshop?
- Benchmark your approach to that of your peers - what are others doing
- Challenge the internal process and enhance where appropriate
- Can be used to aid validation of assessment/quantification of scenarios
- Can help inform resilience testing/ disaster recovery testing

The Scenario Universe Concept



Key Risk Indicator Library

- Repository of over 2,000 insurance relevant KRIs with detailed measurement and usage specifications
- Each of these have been mapped to relevant consortium loss events, newsflashes and scenarios
- Relevant KRIs have been mapped to 38 overarching benchmark scenarios
- The database can be filtered on operational risk category, business function, meta data tags and many other fields
- Each specification can be downloaded in PDF, word or printed



Number	Name [1]	Internal Comparability	Externally comparable	Ease of Use	Nature
10000	Access Rights to Applications by Staff - Frequency of Access Right Reviews	3	Yes	2	Leading, Current, Lagging
10001	Access Rights to Applications by Staff - Number of Reviews beyond Threshold	3	Yes	2	Leading, Current, Lagging
60000	Access Rights to Applications by Staff - Number of Staff with Multiple Access Level Rights	3	Yes	2	Leading, Current, Lagging
60001	Access Rights to Applications by Staff - Number of Staff with Multiple Application Access Rights	3	Yes	2	Leading, Current, Lagging
61178	Access Rights to Applications by Staff - Number of User Maintenance Requests	3	No	3	Current, Lagging
60002	Access Rights to Applications by Staff - Total Number of Reviews	3	No	2	Leading, Current, Lagging
10002	Access Rights to Critical Systems - Frequency of Access Rights Reviews	3	Yes	3	Leading, Current, Lagging
10003	Access Rights to Critical Systems - Number of Customers and Clients with Access	3	No	3	Leading, Current
10504	Access Rights to Critical Systems - Number of Detected Instances of Previous Staff Access Rights not Revoked	3	Yes	2	Current, Lagging

Appendix D - KRI Specification

Definition			
Number:	80113		
Name:	E-Crime and System Security - Number of Losses Due to Hacking and Disruption		
Description:	The total number of losses to the organisation from information technology security violations, unauthorised logins, hackers sniffing web sessions, TCP/IP hacking and other forms of service denial attempts, during the preceding 12 calendar months.		
Nature:	Current, Lagging		
Type:	Loss Frequency		
Causal Type:			
Rationale/Comments:	Indicator quantifies the impact of information technology security breaches.		
Rating:	2 - Internal Comparability	Yes - Externally Comparable	2 - Ease of Use
Common:	No		
Version:	1.1		
Version Release Date:	10/05/2007		
Specification			
Value Format:	Count		
Dimensions:	None		
Buckets:	Indicator values should be divided into value-based buckets reflecting the size of the loss, expressed in the organisation's base currency.		
Bucket Variants:	None specific		
Currency Conversion:	Not applicable		
Measurement Rules:	Include all losses due to information security hacking and service denial during the preceding 12 months, whether from unauthorised logins, hackers sniffing web sessions, TCP/IP hacking or other means. Exclude information technology security issues caused by employees and contractors.		
Underlying Indicators:	None		
Calculation Method:	Count the number of losses meeting measurement criteria. The indicator value should be calculated for each dimensional node listed above, using the aggregation method and scaling rules given below.		
Calculation Formula:	None		
Benchmark Rules:	The indicator value should be scaled for benchmarking by the number of critical systems.		
Aggregation Method:	Simple summation using the dimensional nodes listed.		
Aggregation Rules:	None specific		
Scaling Denominator:	80082 - Critical Systems - Total Number		
Scaling Rules:	The indicator will be scaled by each 10 critical systems. Divide the indicator value by KRI 80082 and multiply the result by 10, rounding the result to 2 decimal places. Aggregate before scaling. Numerator and denominator must be at the same level of aggregation.		

Appendix D - KRI Specification

Guidance	
Usage:	Internal and Benchmarking
Measurement Frequency:	Daily
Reporting Frequency:	Daily
Frequency of Change:	Ongoing
Limitations on Scope:	None specific
Collection Level:	Location
Definition Threshold:	None specific
Variants:	None specific
Direction Information:	Larger number indicates higher risk.
Trend Information:	Increasing number suggests increasing risk.
Control Indicator:	No
Performance Indicator:	No
SoX Indicator:	No
Source:	Information Technology function.
Best Practice Indicator:	No
Best Practice Source:	No
Industry Nature:	Financial Services Generic
Original Release Date:	22/05/2009
Tags:	Cybercrime

Appendix C

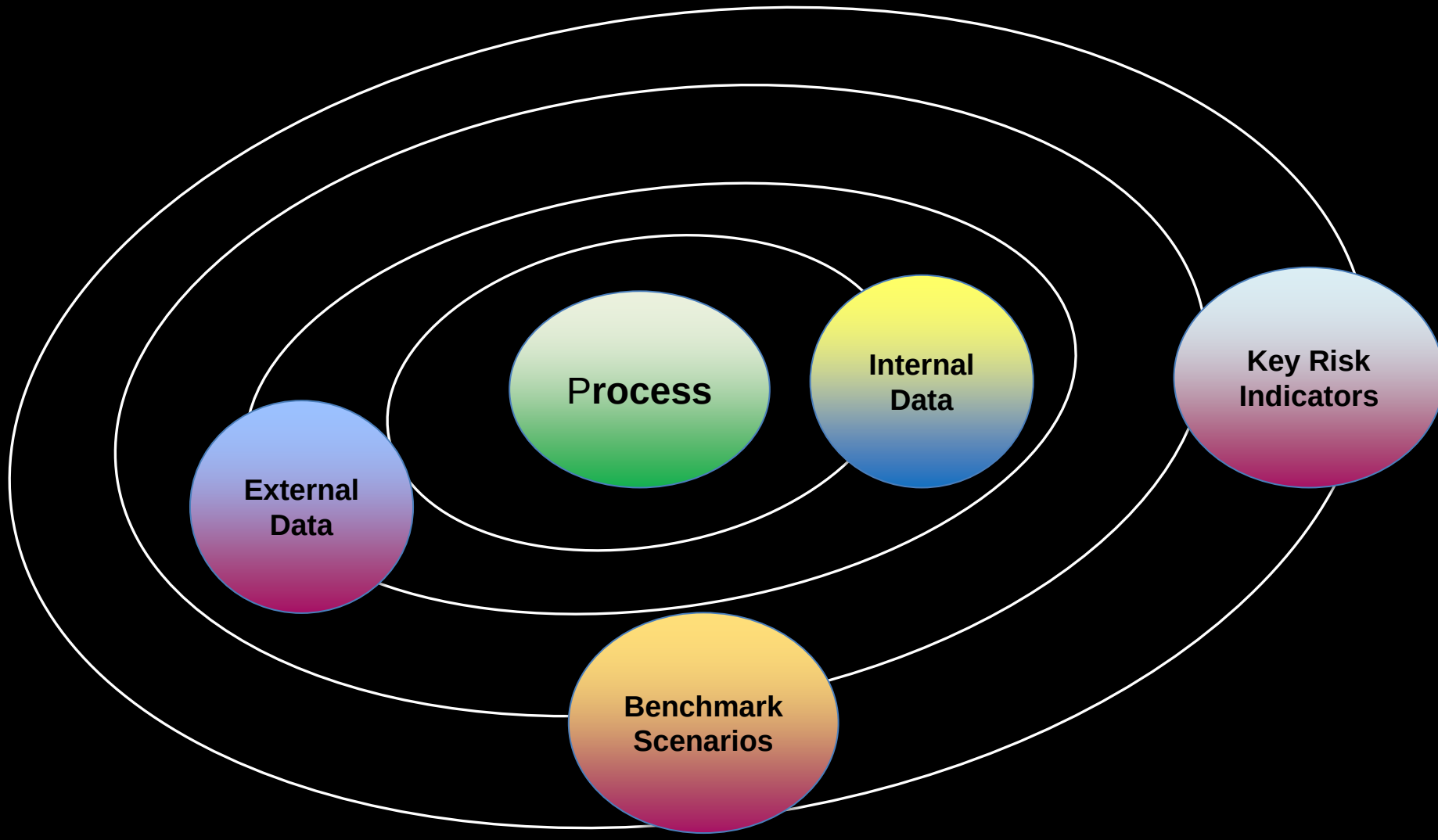
Example Cyber KRI's include:

- E-Crime - Average Value of External Fraud Loss Events per Compromised Customer
- E-Crime - Compromised Account Loss Recovery Rate
- E-Crime - Number of External Fraud and Theft Loss Events due to Compromised Accounts
- E-Crime - Number of Fraudulent E-Mail (Phishing) Instances Detected
- E-Crime - Number of Instances Detected in Market
- E-Crime and System Security - Number of Demilitarised Zone and Firewall Penetrations Detected
- E-Crime and System Security - Number of Losses Due to Hacking and Disruption
- E-Crime and System Security - Number of Unauthorised Website Content Alterations Detected

Uses

- Challenge the completeness and operation of the existing KRI's in place for key relevant scenarios
- Implement new KRI's with detailed usage guidance
- Challenge the internal process and enhance where appropriate
- Mapped scenarios can help firms identify the critical KRI's and prioritise implementation

The Scenario Universe Concept

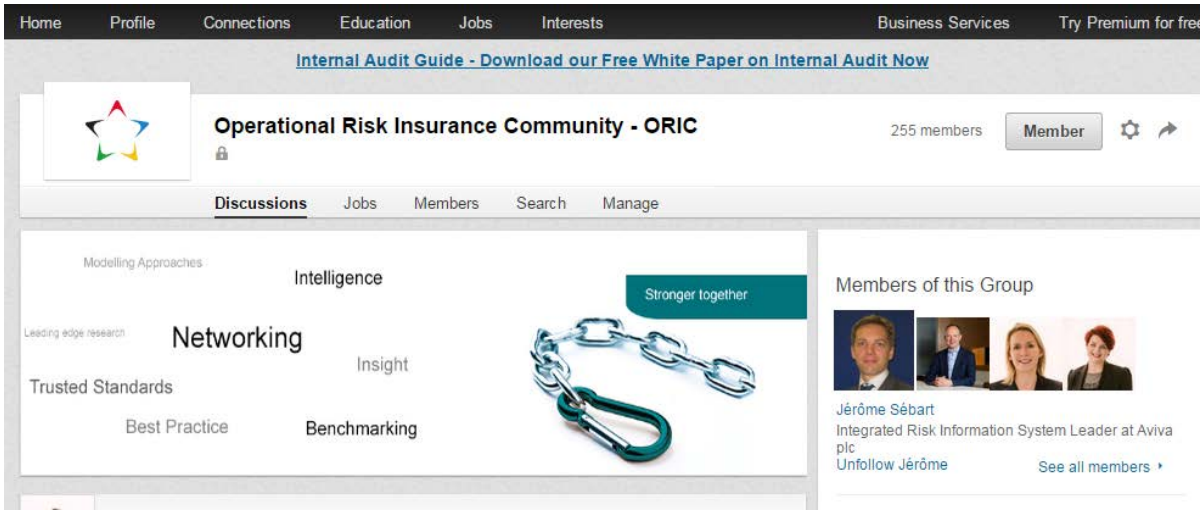


Community

Operational Risk Insurance Community (ORIC)

- We launched our “Operational Risk Insurance Community” group on LinkedIn in June 2014, with the intention of providing a platform for conversations on issues the industry is facing.
- The group now has 255 members from all over the globe
- Join our group today:

Search Operational Risk Insurance Community on LinkedIn



Any questions?

Caroline Coombe – Contact details:

Caroline.coombe@oricinternational.com

Enquiries@oricinternational.com

0207 216 7352

ORIC INTERNATIONAL

Powering risk intelligence