



ORIC
INTERNATIONAL

“It’s all about data”

Caroline Coombe
Chief Executive, ORIC International

Today's agenda

■ **ORIC International**

■ Operational risk

■ Data building blocks for an effective operational risk framework

■ Risk Event Data

■ Scenario analysis

■ Key risk indicators

■ 'Creating value from risk events'

■ Conclusions

ORIC International

- World's leading and largest provider of operational risk event data and analysis for the (re)insurance and asset management industry
- We are a member led and not for profit industry body
- We are a trusted platform for our members to share anonymised information on operational risk, including:
 - Risk event data (near misses and loss events)
 - Scenario benchmarks
 - Capital benchmarks
- We are using our collective expertise, experience and resources to advance operational risk management and measurement
- We are deeply involved in the formulation of best practice for the sector

Our member firms



- ORIC International

- **Operational risk**

- Data building blocks for an effective operational risk framework

- Risk Event Data

- Scenario analysis

- Key risk indicators

- 'Creating value from risk events'

- Conclusions

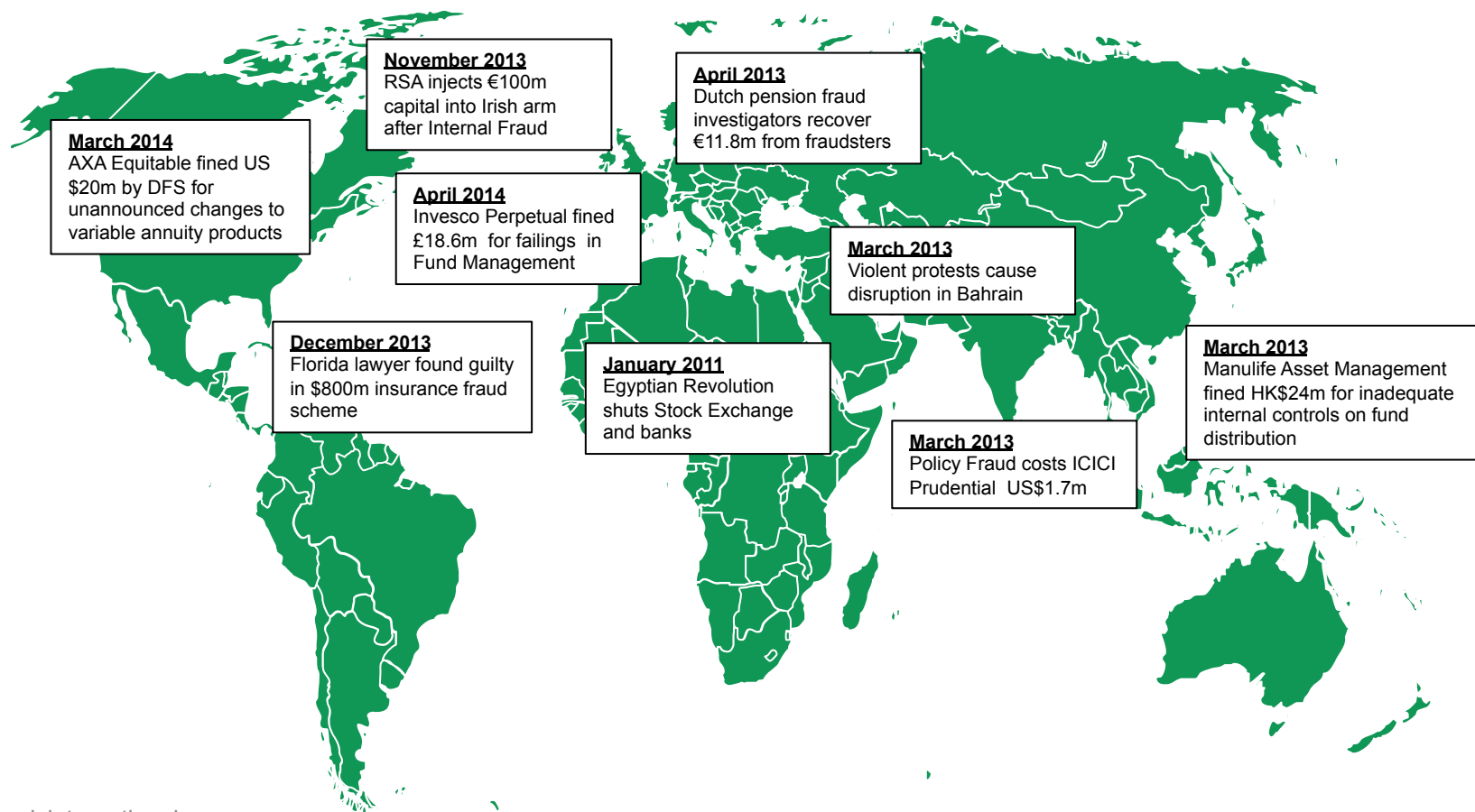
“Of all the types of risk that we face, my personal view is that operational risk is the most pervasive, and in many ways the most nebulous”

**Mark Gregory,
Group Chief Financial Officer,
Legal & General**

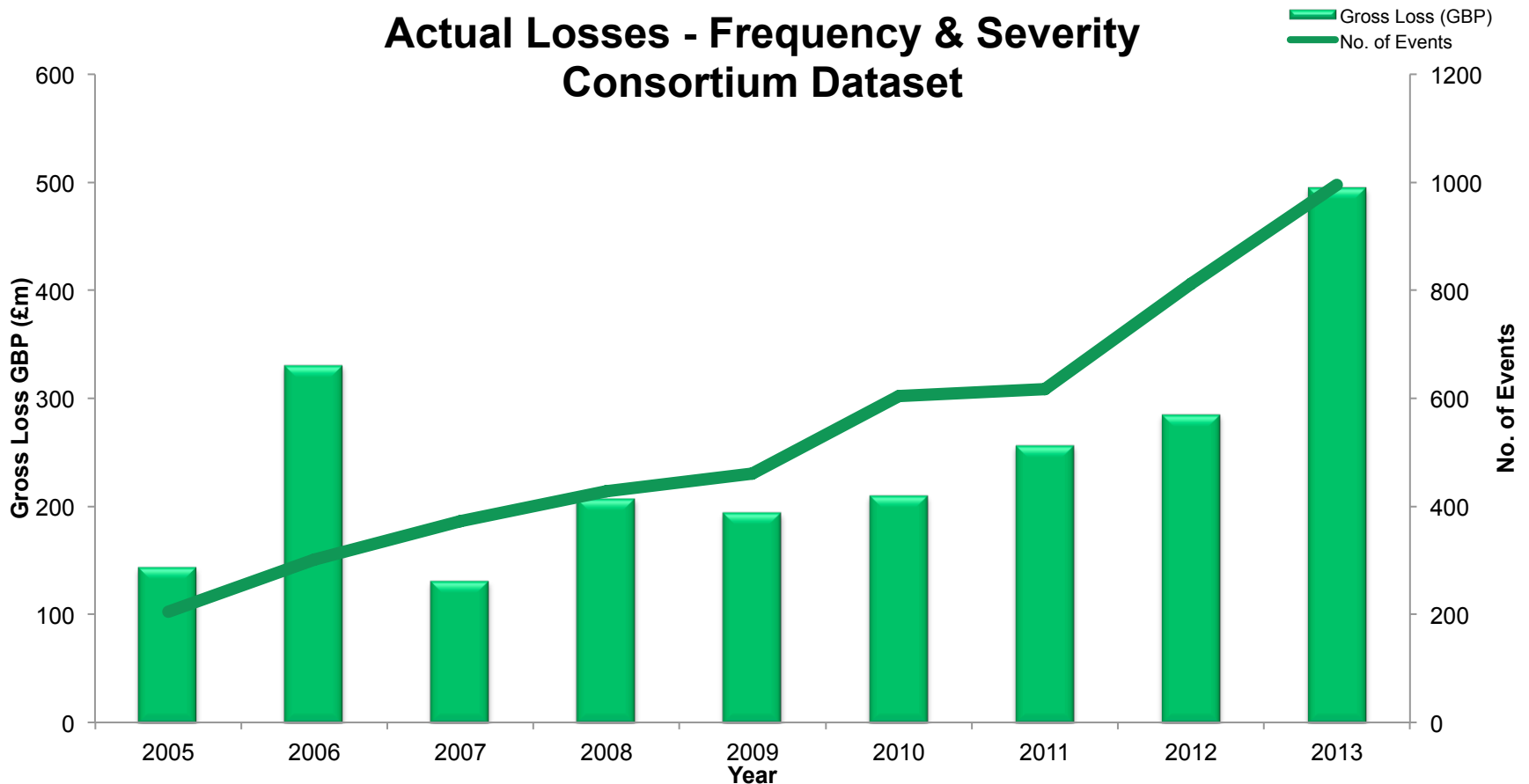
Operational risk happens...

- ING Insurance: Australia's 2nd largest fraud
- 40 year old Rajina Subramaniam worked for ING Insurance in Sydney for 20 years as an accountant
- Embezzled AUD \$45 Million between 2004 and 2010 by transferring suspense account balances and unclaimed client money to personal accounts
- Became known throughout Sydney for her lunch hour shopping sprees, in 2009 alone:
 - Chanel: AUD \$98,452
 - Bulgari: AUD \$3,300,300
 - Paspaley Jewellers: AUD \$7,600,000 (over & above the AUD \$16,000,000 in previous years)
- Reason for the fraud – not valued and respected, Manager delegated everything to her

Everywhere...



And often too...



And when it does it impacts the bottom line

- Largest consortium data-set loss:
 - **£108m GBP**
 - Fund remediation after incorrect product description in marketing literature
- Largest loss in last four quarters:
 - **£72m GBP**
 - Accounting irregularities

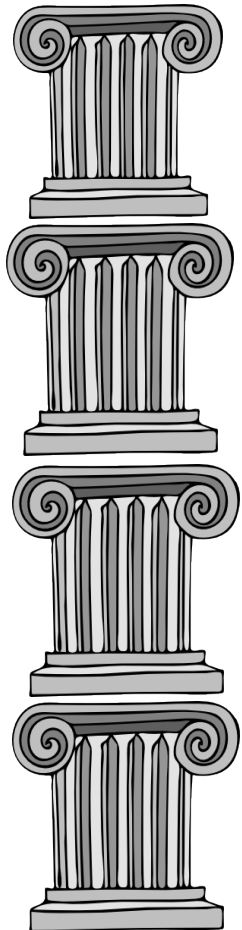
Severity benchmarks from the consortium data-set:

			Average Loss
Q1 2014	Life	Small	£75,349
		Medium	£546,787
		Large	£144,118
	Non-Life	Small	£110,467
		Medium	£260,153
		Large	£488,179

Today's agenda

- ORIC International
- Operational risk
- **Data building blocks for an effective operational risk framework**
- Risk Event Data
- Scenario analysis
- Key risk indicators
- 'Creating value from risk events'
- Conclusions

Operational risk framework



Risk Event Data

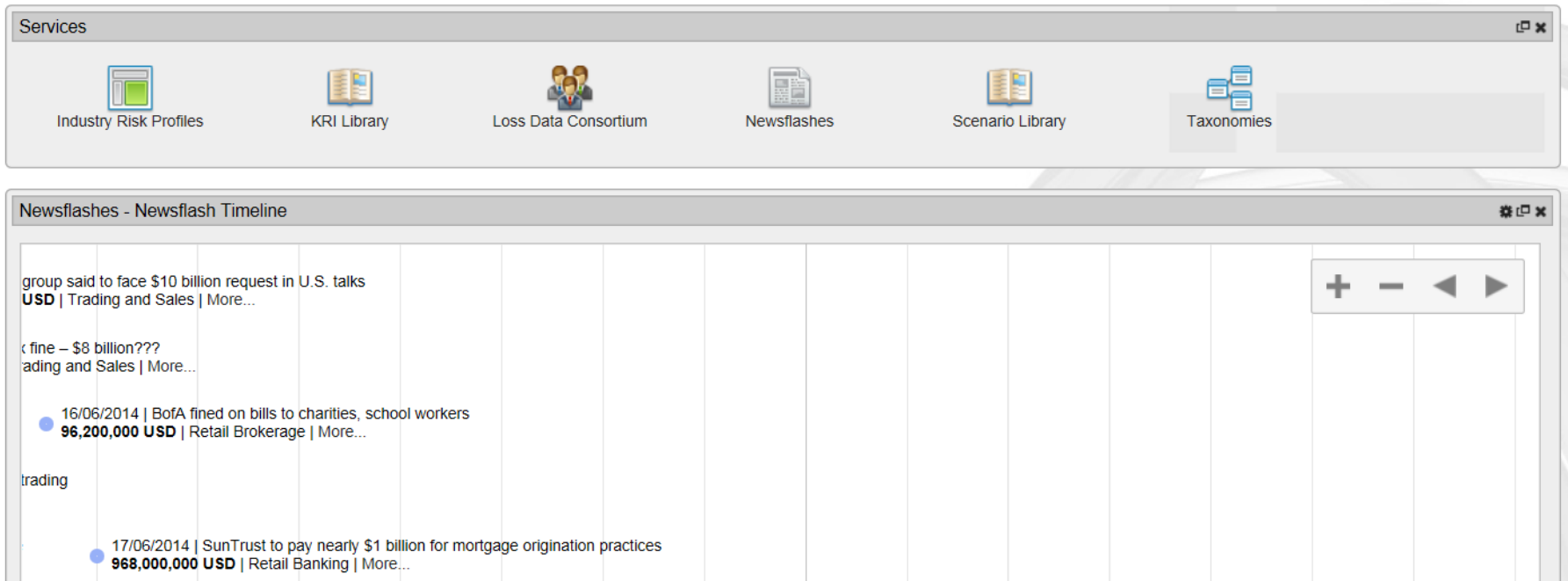
Scenario Analysis

Key Risk Indicators

Risk and Control Self
Assessment's (RCSA)

Your ability to address uncertainty is dependant on 3 key factors:

1. Risk awareness, culture and governance
2. The strength of each individual process
3. How integrated each processes is and how they are used to inform each other



- ORIC International
- Operational risk
- Data building blocks for an effective operational risk framework
- **Risk Event Data**
- Scenario analysis
- Key risk indicators
- 'Creating value from risk events'
- Conclusions

Sources of risk event data

- Internal: Firms own losses and near misses
 - Risk assessment (ORSA) and scenario assessment data
 - Internal incidents, or loss event data
 - Complaints, audit findings, control breaches and near misses
- External: Industry losses and near misses
 - Public sources, such as the press and the internet
 - Commercial vendors of public information
 - Consortium data, derived from participants pooling their internal data and sharing it

What should your firm capture?

Qualitative

- Title
- Event description
- Risk event categories
- Casual types
- Casual description

Qualitative data imperative in enabling firms to learn from loss events, use risk events data as a input to scenario analysis and increase internal data quality.

Quantitative

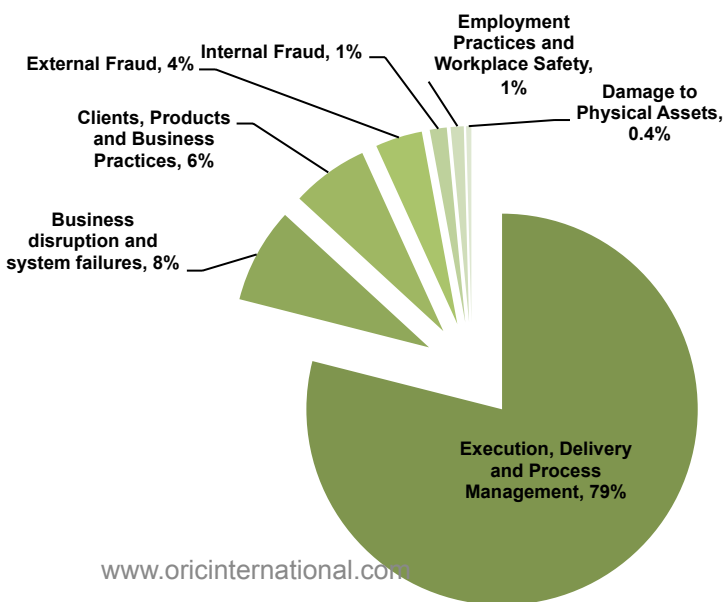
- Occurrence and detection dates
- Gross loss amount
- Recovery amounts
- Direct impacts
- Non direct impacts

Quantitative data is used most commonly as a feed to capital models and frequency and severity benchmarking.

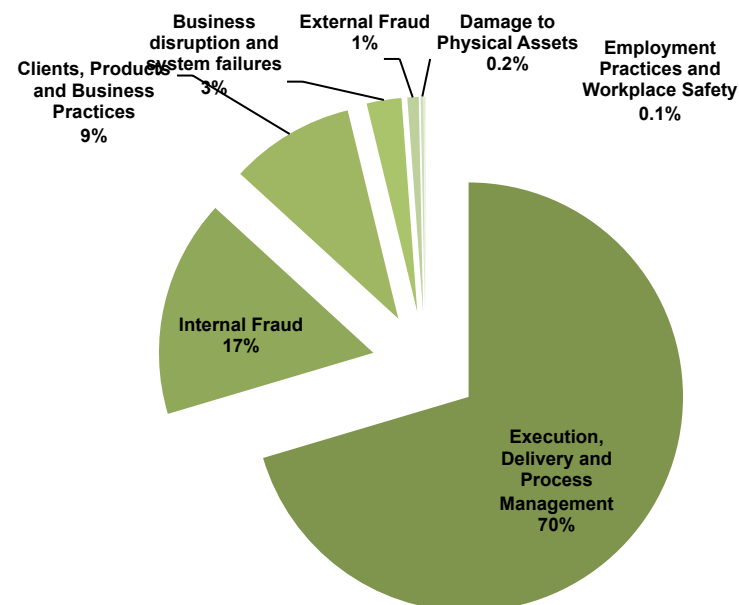
Peer data as a basis for comparison...

	Business disruption and system failures	Clients, Products and Business Practices	Damage to Physical Assets	Employment Practices and Workplace Safety	Execution, Delivery and Process Management	External Fraud	Internal Fraud
% of Events	7.9%	6.4%	0.4%	1.1%	79%	3.9%	1.4%
Highest Single Actual Loss (GBP £m)	£1.9m	£8.9m	£0.8m	£0.2m	£24.1m	£0.9m	£37m
Average Actual Loss (GBP)	£165,467	£733,918	£258,903	£45,917	£443,260	£109,233	£5,815,850

Frequency of Actual Events - 2013



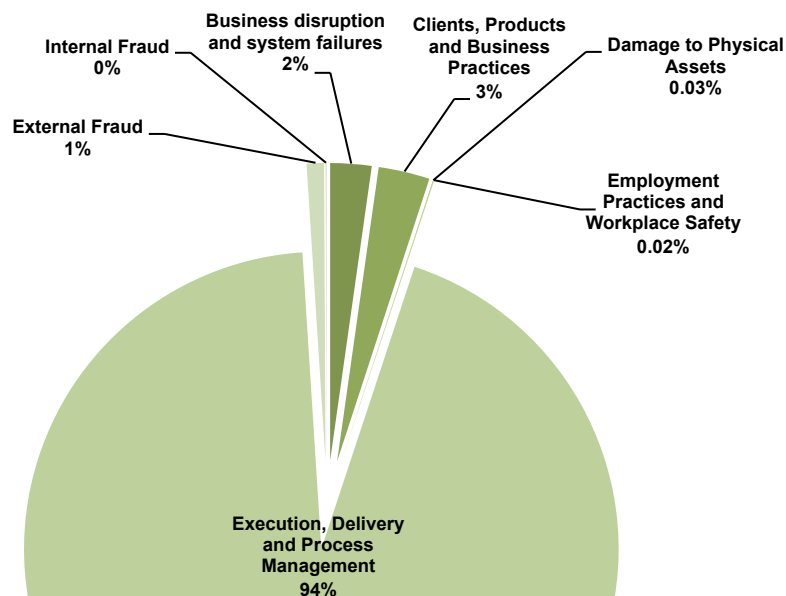
Severity of Actual Events - 2013



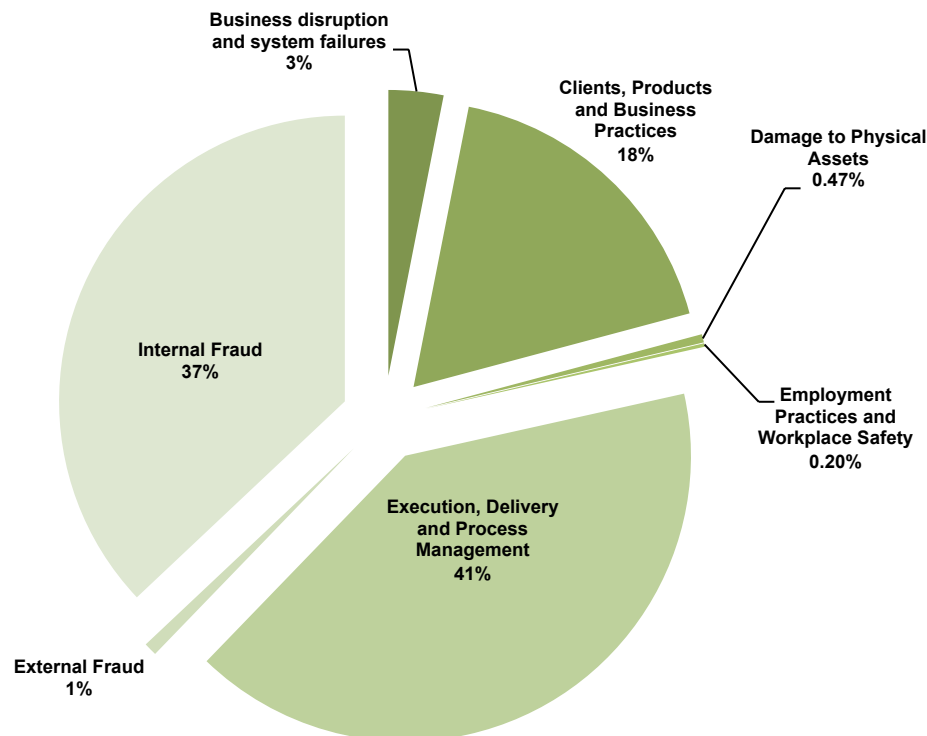
A benchmarking example...

Risk category – Level 1 Analysis

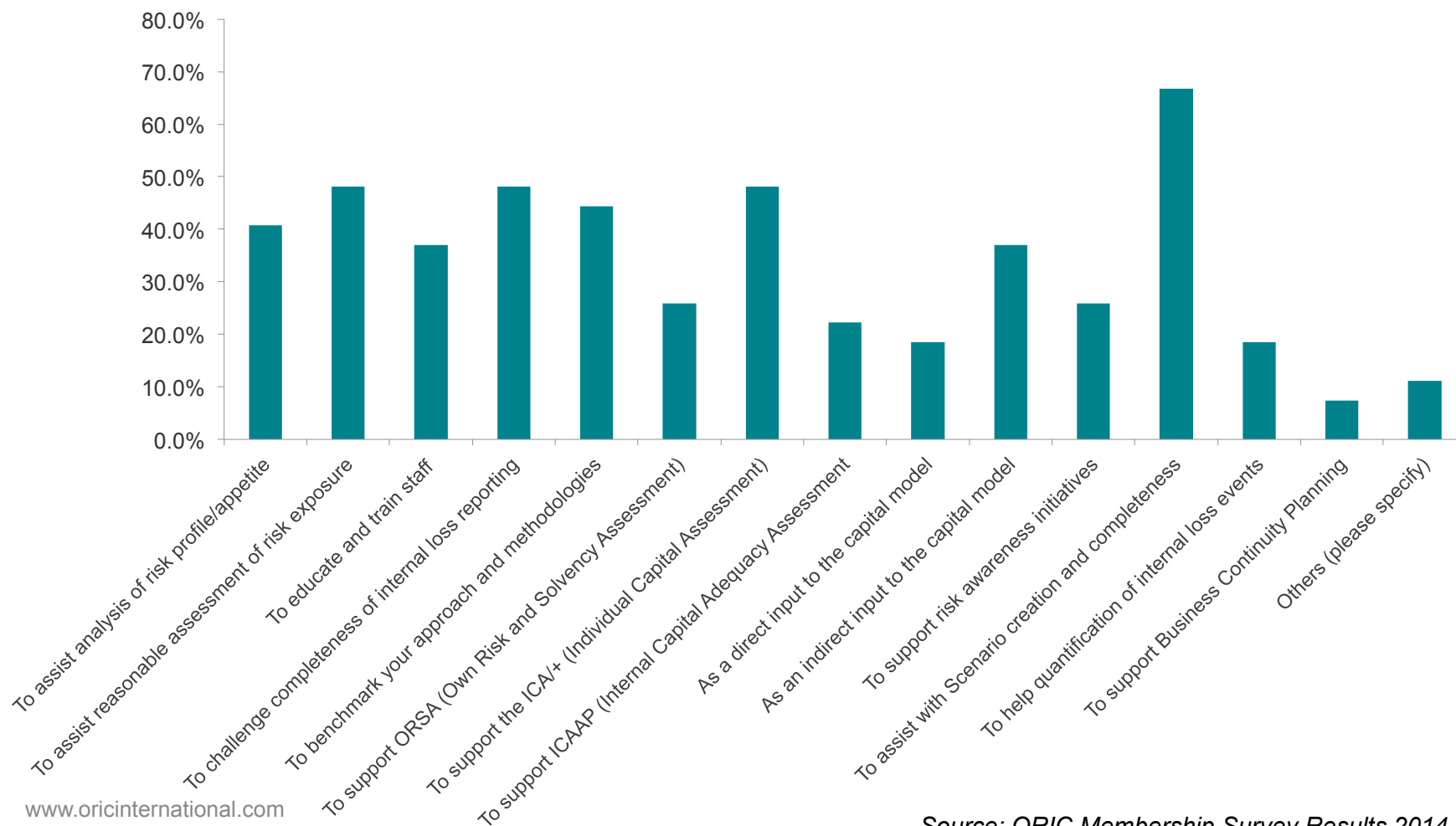
Life



Non-Life



How other firms are using risk event data



- ORIC International
- Operational risk
- Data building blocks for an effective operational risk framework
- Risk Event Data
- **‘Creating value from risk events’**
- Scenario analysis
- Key risk indicators
- Conclusions

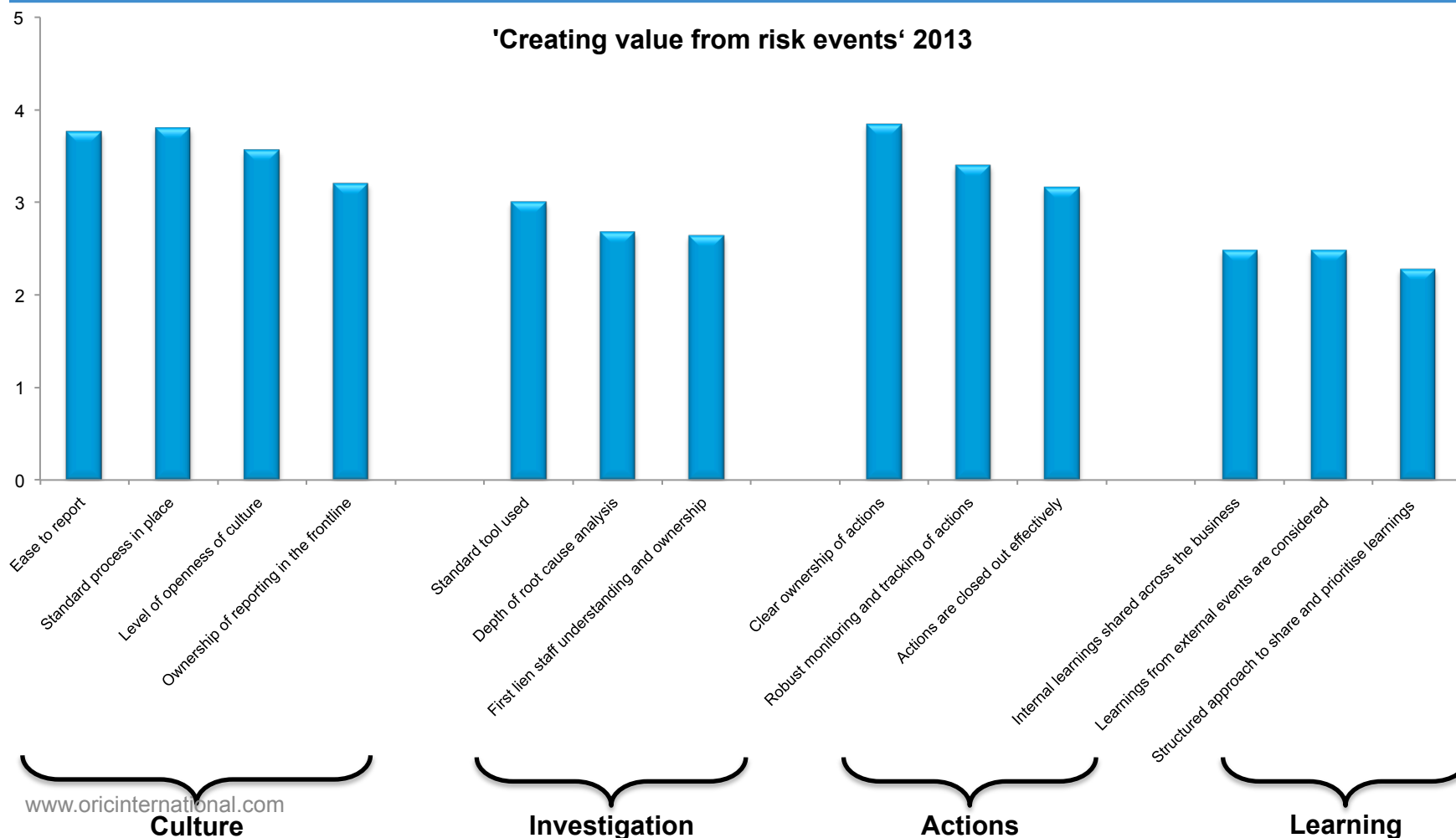
ORIC & Oliver Wyman Study 2013

“Organisations which place a strong focus on risk event reporting, analysis and learning actively reduce operational risk losses”

The 4 things you need to get right

1. Creating an open culture that encourages reporting
2. Event investigation and analysis, including impact assessment
3. Managing actions
4. Learning and continuous improvement

Areas to focus on



Where is your firm now?

	Reactive	Compliant	Proactive	High reliability
Open environment for reporting	<ul style="list-style-type: none"> Only significant risk events are reported Lack of leadership involvement Inconsistent reporting processes Fear of blame/ reprimand impedes reporting People are unsure what to report and why Reporting delegated to the 2nd line Near misses not reported 	<ul style="list-style-type: none"> Coherent process for people to report events Most events reported Key people are risk aware Key people understand how to report a risk event Little focus on near miss reporting 	<ul style="list-style-type: none"> Everyone feel encouraged to report events Simple standardised company-wide approach to reporting Ownership of reporting at 1st line Selected staff at 1st line of defence staff are focused on risk Staff understand the need to report near misses. >50% are reported 	<ul style="list-style-type: none"> Single, simple approach to capture enterprise-wide risks Everyone understand current and potential risks they face Everyone understands the need to report risk events and do so directly Open, learning culture sees events as an opportunity to improve Near misses actively reported in order to reduce frequency of loss events
Risk Event analysis, investigation and impact assessment	<ul style="list-style-type: none"> Focus on addressing recovery from loss events Leadership seek to identify responsibility and blame Root cause analysis (RCA) not conducted 	<ul style="list-style-type: none"> Root Cause Analysis (RCA) conducted for priority events Focus on controls, processes and systems – not behaviours Ad hoc and inconsistent approach to RCA - few standard tools Little trained investigative capability 	<ul style="list-style-type: none"> Clear thresholds for Root Cause Analysis (RCA) Standard, proven tools and approaches used to conduct RCA Behavioural root causes always sought Strong trained capability to conduct RCA Top leadership reviews causes of major events 	<ul style="list-style-type: none"> Deep Root Cause Analysis (RCA) for key events and major near misses Analysis identifies trends and causes from volume lesser events All leaders are seen to engage in RCA Focus on behaviours (why people acted that way) Leadership, behavioural and cultural issues confronted Quality assurance of investigations through peer and 3rd line review
Action management	<ul style="list-style-type: none"> Actions for most loss events are not monitored or followed up Follow-up for major events is on ad hoc basis 	<ul style="list-style-type: none"> Actions often derived so that they can be delivered rather than make a difference Actions are managed, monitored and closed Approach and tools for action management are not consistent across company 	<ul style="list-style-type: none"> Actions derived to make a difference Actions are prioritised based on resources available and risk appetite Actions clearly tracked and only closed on evidence Top leadership review actions for major events 	<ul style="list-style-type: none"> Action management process integrated into company-wide continuous improvement approach Actions may involve replacing existing controls that are not cost effective, not just adding additional controls
Learning and continuous improvement	<ul style="list-style-type: none"> No systematic approach in place to learn from internal or external risk events Learnings tend to be ad hoc and rely often on informal networks 	<ul style="list-style-type: none"> Changes to policies and procedures occur in response to significant internal risk events Learnings not always shared across all relevant parts of the company Review of major external risk events is not systematic 	<ul style="list-style-type: none"> Processes in place to prioritise and share learnings across the company from internal risk events Learnings are derived from external risk events Appropriate ORIC data shared with 1st line Multiple channels used to engage staff in learnings The 3rd line review learning effectiveness 	<ul style="list-style-type: none"> Learnings from loss events and near misses used to deliver year on year reductions in risk exposure Rigorous approach optimise behaviours and controls based on learning from internal and external events Proactive sharing and learning across the industry to reduce sector-wide operational and reputational risks

-
- ORIC International
 - Operational risk
 - Data building blocks for an effective operational risk framework
 - Risk Event Data
 - 'Creating value from risk events'
 - **Scenario analysis**
 - Key risk indicators
 - Conclusions

Scenario Analysis

- Internal and external data is a key input
 - Benchmarking
 - Sense-checking
- Also able to use internal/external data to inform the scenario technical specification and thought process
 - Inform frequency/severity assessments
 - Use of direct/indirect impacts
 - Validation of outputs
- ORIC's Scenario Library contains over 400 detailed scenarios covering all aspects of operational risk

External risk event data and severity estimates

- UK operation of Zurich Insurance fined by the FSA (Financial Services Authority) for losing the personal details of 46,000 customers
- It was the highest fine levied on a single firm for data security failings
- Data (including bank account/credit card details) went missing in transit to a data storage centre in South Africa in August 2008
- However the loss wasn't uncovered until a year later
- Agreed to settle at an early stage in the investigation, which reduced the fine by 30%

How much did this cost them?

- £100,000 - £500,000
- £500,001 - £1,000,000
- £1,000,001 - £3,000,000
- £3,000,001+

How much would this have cost your firm?

Ask yourself :

- Is the event relevant to my firm?
- Could we be exposed to a similar event?
- Which functions would be affected?
- What would the impact be?
- How would our control environment respond?
- How effective do we think our internal controls are?
- Do we need to take any action?
- Are there any patterns or trends in our internal or external data?
- Can we refine existing key risk indicators or develop new ones to help monitor the risk?

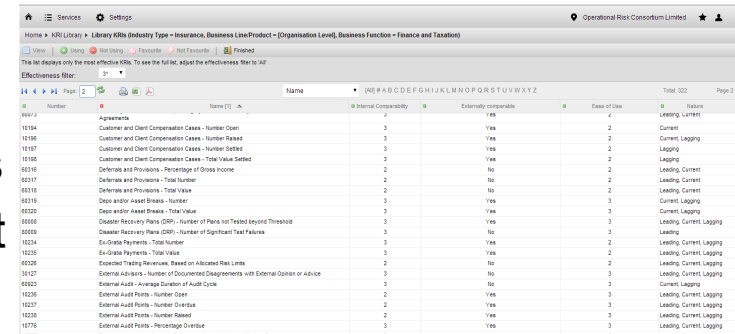
-
- ORIC International
 - Operational risk
 - Data building blocks for an effective operational risk framework
 - Risk Event Data
 - 'Creating value from risk events'
 - Scenario analysis
 - **Key risk indicators**
 - Conclusions

Key Risk Indicators

- Increased interest in topic as move towards more structured operational risk approach (e.g. Bayesian Networking)
- Can use risk event data (Internal & External) to inform thresholds
 - Internal: Find appropriate thresholds internally based on existing processes and controls
 - External: Benchmark choices made using Internal Data and use for systemic/external event KRIs
- Outputs can be used to inform and guide your scenario planning and assessment programs
 - Where to target assessments
 - Allows assessment of existing control frameworks

Key Risk Indicators

- ORIS – KRI Library
 - Approximately 2,500 KRIs in searchable library
 - Mapped to relevant scenarios/loss events
 - Can create firm-specific library of relevant KRIs
- Detailed KRI specifications including:
 - Descriptive information
 - Measurement & calculation information
 - Relevant risk categories and business functions
 - Much more...



Name	Internal Competency	Externally Competent	Base of Use	Status
10104 Customer and Client Compensation Cases - Number Open	3	Yes	2	Current
10106 Customer and Client Compensation Cases - Number Raised	3	Yes	2	Current Lagging
10107 Customer and Client Compensation Cases - Number Settled	3	Yes	2	Lagging
10108 Customer and Client Compensation Cases - Total Value Settled	3	Yes	2	Lagging
10216 Deferrals and Provisions - Percentage of Gross Income	2	No	2	Leading Current
10217 Deferrals and Provisions - Total Number	2	No	2	Leading Current
10218 Deferrals and Provisions - Total Value	2	No	2	Leading Current
10219 Deep and/or Asset Breaks - Number	3	Yes	3	Current Lagging
10220 Deep and/or Asset Breaks - Total Value	3	Yes	3	Current Lagging
10221 Disaster Recovery Plans (DRP) - Number of Plans not Tested beyond Threshold	3	Yes	3	Leading Current Lagging
10222 Disaster Recovery Plans (DRP) - Number of Significant Test Failures	3	No	3	Leading
10224 Ex-Gratia Payments - Total Number	3	Yes	2	Leading Current Lagging
10225 Ex-Gratia Payments - Total Value	3	Yes	2	Leading Current Lagging
10226 Exposed Trading Securities - Based on Allowed Risk Limits	3	No	3	Leading Current Lagging
10227 External Advisers - Number of Documented Disagreements with External Opinion or Advice	3	No	3	Leading Current Lagging
10228 External Audit - Average Duration of Audit Cycle	3	No	3	Current Lagging
10229 External Audit Points - Number Open	2	Yes	3	Leading Current Lagging
10230 External Audit Points - Number Overdue	2	Yes	3	Leading Current Lagging
10231 External Audit Points - Number Raised	2	Yes	3	Leading Current Lagging
10232 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10233 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10234 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10235 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10236 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10237 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10238 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10239 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10240 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10241 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10242 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10243 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10244 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10245 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10246 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10247 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10248 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10249 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10250 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10251 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10252 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10253 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10254 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10255 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10256 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10257 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10258 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10259 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10260 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10261 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10262 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10263 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10264 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10265 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10266 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10267 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10268 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10269 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10270 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10271 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10272 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10273 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10274 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10275 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10276 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10277 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10278 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10279 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10280 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10281 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10282 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10283 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10284 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10285 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10286 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10287 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10288 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10289 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10290 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10291 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10292 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10293 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10294 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10295 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10296 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10297 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10298 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10299 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging
10300 External Audit Points - Percentage Overdue	3	Yes	3	Leading Current Lagging

KRI Name	Description	Rationale	Suggested Frequency
System Security - Number of Open High Severity IT Security Log Entries	The number of open IT security events deemed to be high severity, at the point of measurement.	Indicator measures exposure to technology security.	Daily

-
- ORIC International
 - Operational risk
 - Data building blocks for an effective operational risk framework
 - Risk Event Data
 - 'Creating value from risk events'
 - Scenario analysis
 - Key risk indicators
 - **Conclusions**

Conclusions



'I never guess. It is a capital mistake to theorise before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.'

Sir Arthur Conan Doyle

Questions?

Contact us

Web: www.oricinternational.com

Email: enquiries@oricinternational.com

Tel: +44 (0) 207 214 7355



ORIC
INTERNATIONAL

Powering risk intelligence