Welcome

Imran Shah

Head of Risk Europe,
Travelers Insurance

TRAVELERS

Profiling Risk Best Practice Webinar

Disclaimer

- This presentation is intended for discussion purposes only and does not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenter individually and, are not the opinion or position of any company, governing body, professional body, consultancy or software/database consortium or vendor.
- This presentation summarises a hypothetical risk framework linked to UK financial services regulatory reporting and does not imply endorsement by any company, governing body, professional body, consultancy or software/database consortium or vendor.
- The presenter does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

TRAVELERS

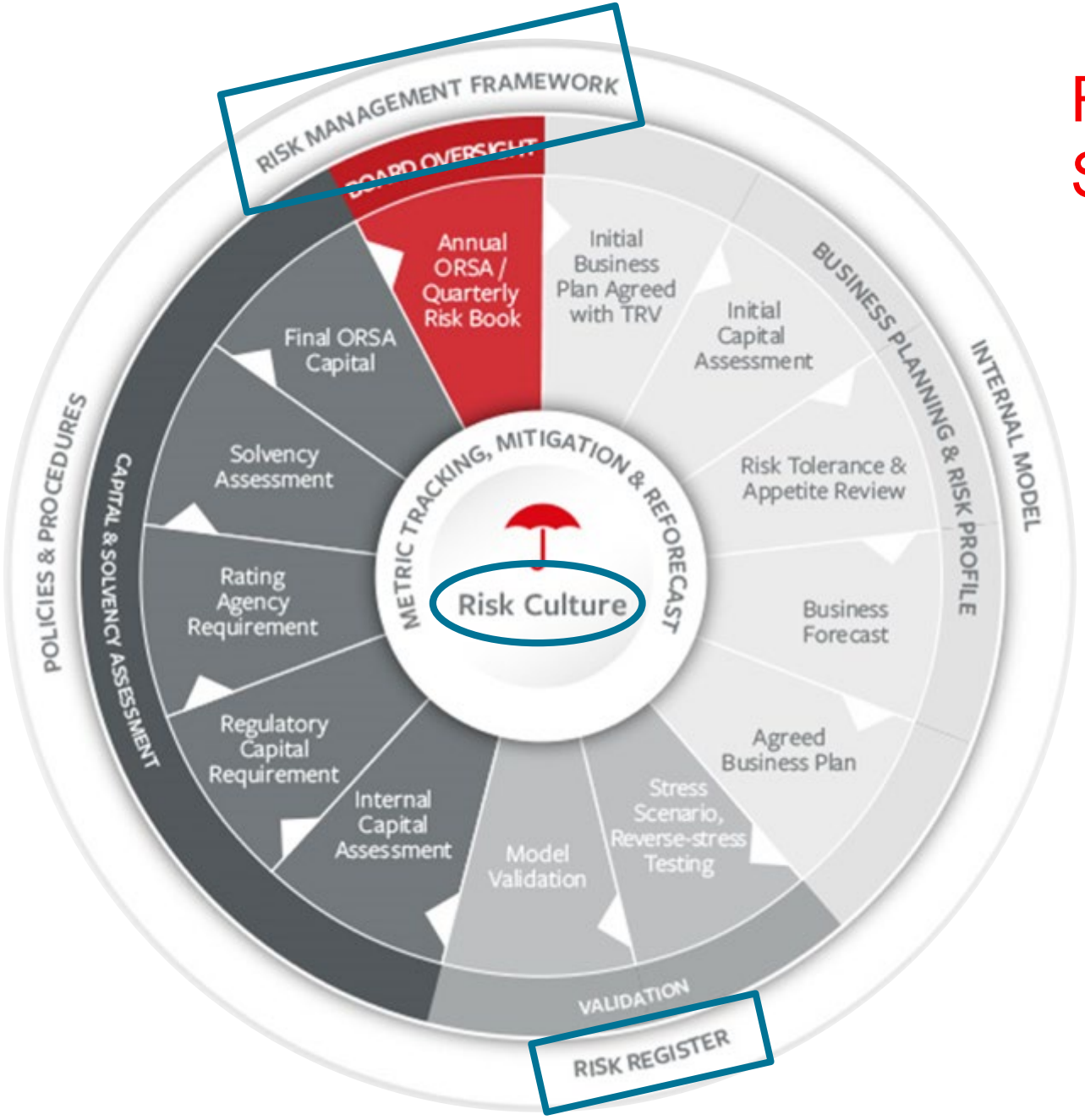
A Day in the Life of an Insurance CRO/Head of ERM

Travelers Group 2019 Year End
A Position of Strength Planning for the Unknown & Unforeseeable

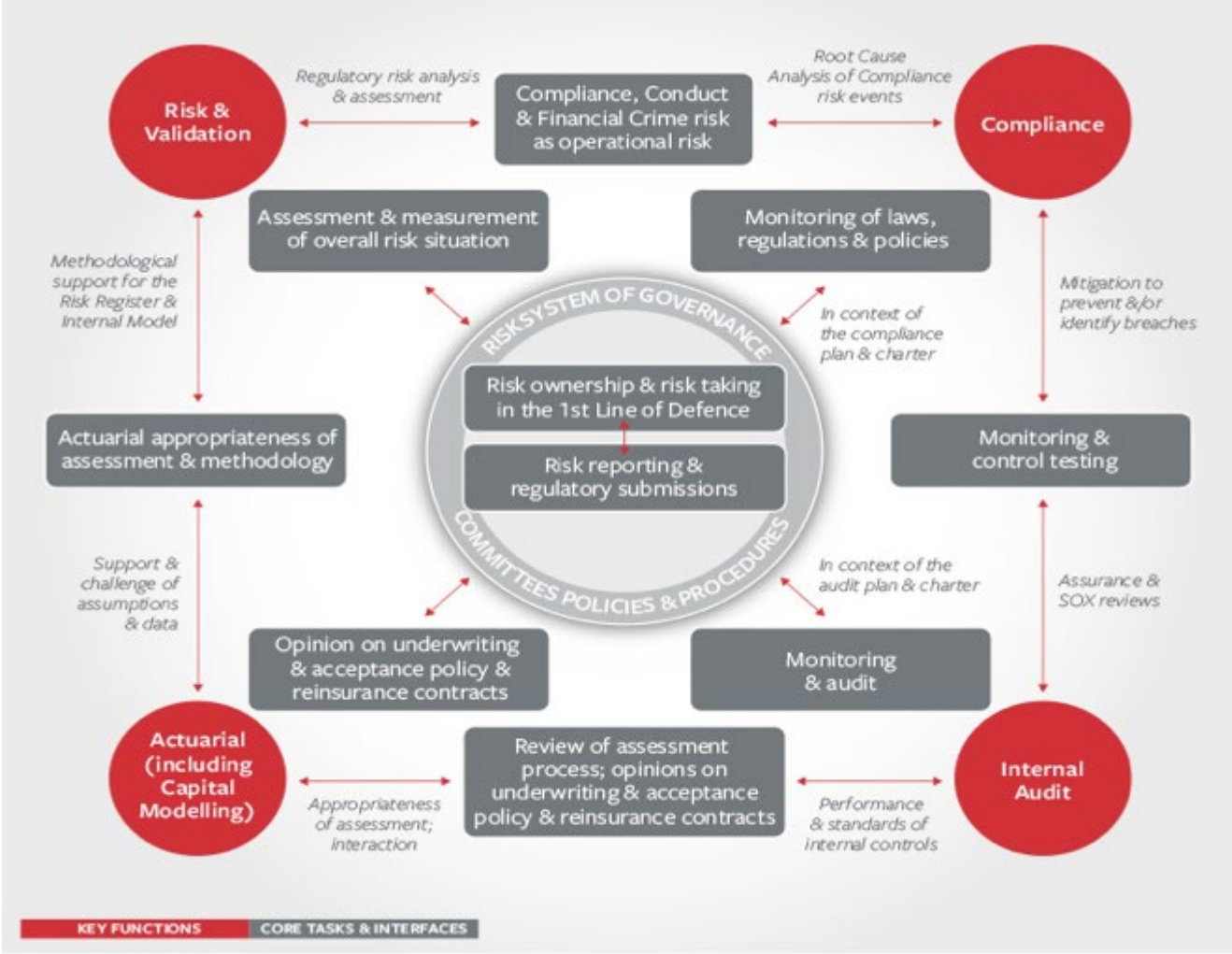
- Over 160 years of experience as a leading property and casualty insurer.
- Business mostly in United States, Canada, United Kingdom and Republic of Ireland. Approximately 30,000 employees.
- Record net written premiums of more than $29 billion. Over the past four years grew net written premiums at a compound annual rate of 5%.
- Net income of $2.6 billion, an increase of 4% over the prior year, and return on equity (ROE) of 10.5% (industry average 8.2%). Travelers ROE has significantly outperformed the average ROE for the industry in each of the past 10 years.
- 14th consecutive year in which Travelers increased its dividend. Returned $2.4 billion of excess capital to shareholders through dividends and share repurchases.
- High-quality investment portfolio generated strong net investment income of $2.1 billion after-tax.
- Consolidated expense ratio has improved by more than 7%, from an average of 31.9% during the period from 2010 to 2015 to 29.6% for 2019.
- Distribution mostly through independent agents and brokers with whom we have long and excellent relationships.
- Member of Dow Jones Industrial Average, added June 8th 2009.

TRAVELERS

Risk & Capital: Insurance Sector's Core Competency



ERM in Travelers Europe



Risk Requirements

from regulators, rating agencies &
professional bodies

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Coimisiún
Cosanta Sonraí
Data Protection
Commission

STANDARD
&POOR'S

TRAVELERS

The Risk Conundrum

The UK Corporate Governance Code

O. The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve it's long-term strategic objectives.

28. The board should carry out a robust assessment of the company's emerging and principal risks.[9] The board should confirm in the annual report that it has completed this assessment, including a description of its principal risks, what procedures are in place to identify emerging risks, and an explanation of how these are being managed or mitigated.

29. The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

9 - Principal risks should include, but are not necessarily limited to, those that could result in events or circumstances that might threaten the company's business model, future performance, solvency or liquidity and reputation. In deciding which risks are principal risks companies should consider the potential impact and probability of the related events or circumstances, and the timescale over which they may occur.

There is little in the form of detailed regulatory operational risk requirements and this presents an **opportunity** to risk functions to tailor it to add value.

riskcoalition.org.uk

- The Risk Coalition's objectives for this principles-based guidance are to:
- establish a common understanding of the purpose, role and activities of the board risk committee and risk function;
- provide a benchmark against which board risk committees and risk functions can be assessed objectively;
- raise the general standard of risk governance and oversight practice within UK financial services; and
- fill the gap in principles-based good practice risk guidance whilst recognising the presence of detailed regulation.
- Published in December 2019.

The Risk Problem

- Can be Complex
- Different Perspectives & Duplication
- Diverse Professional Standards & Definitions
- Bias / Heuristics / Assumptions

Types of Risk Management

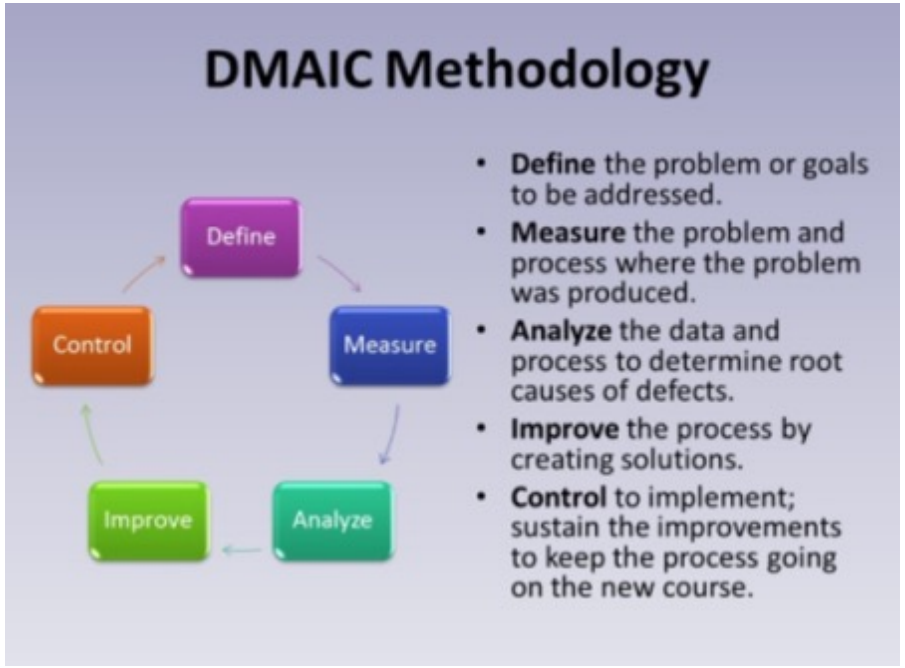
1. Enterprise Risk Management:
2. Operational Risk Management
3. Financial Risk Management
4. Market Risk Management
5. Credit Risk Management
6. Quantitative Risk Management
7. Commodity Risk Management
8. Bank Risk Management
9. Non-profit Risk Management
10. Currency Risk Management
11. Project Risk Management
12. Integrated Risk Management
13. Technology Risk Management
14. Software Risk Management
15. IT Risk Management

- Lawyers
- Accountants
- Actuaries
- Chartered Financial Analysts
- Underwriters
- Claims
- IT / Information Security
- & Others

- COBIT: Control Objectives for Information and Related Technologies
- ITIL: Information Technology Infrastructure Library
- ISO (31000; 73; 22301; 31010; 27002; 27036; 19011; 31004; 27005; 30121; 3494; 13569; 19011; 22307; 27040; 28004; 27018; 30104; 27033; 27035)…
- Solicitors Regulatory Authority (or equivalent)
- PCI: Payment Card Industry
- TAS; IRM; FRM; FERMA; CFA; IOR; CII….
- COSO
- SoX
- & there's a lot more..

TRAVELERS

How To (Potentially) Develop the Risk Solution



Source existing detailed operational & Board risk information.

Structure it & define materiality.

Taxonomy - from Greek *taxis*, meaning arrangement or division, and *nomos*, meaning law - is the science of **classification according to a predetermined system**, with the resulting catalogue used to provide a **conceptual framework for discussion, analysis or information retrieval**. In theory, the development of a good taxonomic classification takes into account the importance of separating elements of a group (taxon) into subgroups (taxa) that are **mutually exclusive and unambiguous, and taken together, include all possibilities**. In practice, a good taxonomy should be simple, easy to remember and use.

The Travelers Europe Answe

‘Risk Profiling’

Example of the Insurance Sectors Top Risks

Top Risk		Description	Source
1	Insurance	Underwriting, reinsurance, reserving, or claim activity, result in a material, or potentially material, impact on planned financial performance.	Insurance Risk Policy
2	Investment & Market	Fluctuations in the market price of securities, derivatives, or other financial instruments.	Investment & Market Risk Policy
3	Operational	Failure of processes, people, systems, and from external events.	Operational Risk Policy
4	Credit	Another party fails to perform its debt obligations or fails to perform them in a timely fashion.	Credit Risk Policy
5	Liquidity	Liabilities cannot be met when they fall due, or can only be met at an uneconomic price.	Liquidity Risk Policy
6	Strategic	Current and prospective impact on earnings or capital arising from business decisions or industry changes.	Group Risk Policy

TRAVELERS

FS Operational Risk Taxonomy

Operational
Compliance, Legal & Third Parties
Conduct
Data Management & Reporting
Employee & Employment Practices
Financial Crime
Infrastructure, Security & Change

ERM is a collection of processes whereby Travelers systematically ensures that the risks it faces, when aggregated, are within tolerance (or appetite) & considers mitigating action in view of the cost/benefit.

Identify the other risk approaches and specialists. Link other specialist frameworks with ERM e.g. Legal, Sales/Distribution, HR, IT/Information Security, Compliance, Change, Marketing.

This is a high level Board view that applies to financial services & some risks can be considered for other sectors.

Risk Functions are responsible for developing the detail (in the insurance sector we are a Key Function).

TRAVELERS

Risk Identification: Operational Risk

Level II Risk	Level III Risk & Description
3.1 Compliance, Legal & Third Parties	**3.1.1 Change in Regulation or Law:** Modification of rules or law, &/or interpretations by the courts, &/or incorrect legal advice, impacts the business.
	3.1.2 Compliance: Regulatory deficiency that may result in enforcement action, loss of trading license &/or reputational damage.
	3.1.3 Governance: Existence of a governance structure & the evidence of structure by means of Terms of Reference, guidelines & procedures.
	3.1.4 Legal Dispute & Contract: A potential disagreement with a third party concerning the terms of an enforceable arrangement (excludes insurance risk).
	3.1.5 Suppliers & Partners: A third party (includes brokers & outsource providers) fails to deliver the expected level of service.

Risk Identification: Operational Risk

Level II	Level III Risk & Description
3.2 Conduct	**3.2.1 Complaints:** Failure to identify or handle in a way that is expected by the regulator, any expression of dissatisfaction, whether oral or written, whether justified or not, from or on behalf of an eligible complainant about the provision of, or failure to provide, a product or service.
	3.2.2 Customer Service: The Company does not deliver what the customer expects &/or adequate maintenance of customer needs / expectations, or customer outcomes may be unfair.
	3.2.3 Literature Defects: Erroneous, misleading, ambiguous or unenforceable terms & conditions result in ambiguity for the customer &/or unintended risks being covered.
	3.2.4 Mis-Selling: Deliberate, reckless, or negligent sale of products or services in circumstances where the contract is misrepresented, or customers are sold products & services that do not fit their needs (suitability).
	3.2.5 Product & Service Development: Deficiencies in product development, design or approval.

Risk Identification: Operational Risk

Level II	Level III Risk & Description
3.3 Data Management & Reporting	**3.3.1 Data Supplied by a Partner is Deficient**: Third party (includes broker or outsourcer) provides inaccurate, or inadequate, data.
	3.3.2 Errors, Gaps or Delays in Accounting, Financial or MI: Inaccurate, misleading or false information is reported to governing bodies or others.
	3.3.3 Handling of Sensitive or Confidential Data: Unauthorised use, or access, of restricted information. Sensitive details of customers, employees, or the business are available to unintended parties.
	3.3.4 Manual Data Handling & Computation: Deficient data entry, or data migration process lead to inaccurate inputs.

Risk Identification: Operational Risk

Level II	Level III Description
3.4 Employee & Employment Practices	**3.4.1 Resources**: Teams are unable to execute their duties &/or carry out their role due to lack of skills, competencies, authorisation, capacity or capability.
	3.4.2 Employee Engagement: Employees have clarity of purpose & understand how their role contributes to the business. The work environment encourages involvement & motivates.
	3.4.3 Employee Litigation: Formal action by an (ex)employee leads to financial compensation &/or reputational impact.
	3.4.4 Talent & Succession: The ability to attract & retain high performers &/or lack of succession planning leads to a significant impact on the business.

Risk Identification: Operational Risk

Level II	Level III Description
3.5 Financial Crime	**3.5.1 Bribery & Corruption**: Failure to prevent employees (or associated persons) committing offences to win, or keep business, or gain advantage. Employees giving, offering, requesting or receiving benefits in an attempt to improperly influence internal or external business decisions.
	3.5.2 External Fraud: A deliberate act by external agent(s) puts The Company's assets at risk.
	3.5.3 Internal Fraud: Deceit involving employee(s), either acting individually or attempting to collude with a third party.
	3.5.4 Money Laundering: Engaging or assisting in the concealment of the origins of illegally obtained money.
	3.5.5 Sanctions: Deliberate or negligently transacting with parties listed on trade, financial sanctions & export control lists. The identification & disclosure of suspicious transactions & activities.

Risk Identification: Operational Risk

Level II	Level III Description
3.6 Infrastructure, Security & Change	**3.6.1 Application, Infrastructure or Network**: Business operations are materially impacted by the underperformance or failure of IT applications &/or infrastructure.
	3.6.2 Business Continuity & Disaster Recovery: Unexpected discontinuation of business processes, including access to facilities, following a natural or man-made catastrophe (e.g. act of war, pandemic, critical IT failures, industrial accident or failure of Business Continuity Plans/Disaster Recovery).
	3.6.3 Project & Change Management: A material project fails or is delayed &/or is not delivering as planned. Inappropriate change programmes are selected for implementation &/or shared resources are managed inefficiently.
	3.6.4 Systems Security, Loss or Damage to Assets: Accidental or deliberate destruction or corruption of information or physical assets (includes mobile devices).

Risk Drivers

Also known as threats or potential causes of risk.

- Risk drivers can amplify risks and/or alter the relationship/correlation between them over time.
- Risk drivers tend to headline the ways it is perceived that risk performance could (or would) fluctuate.
- Prioritise risk drivers frequently as they change and/or the business evolves.

Key Risk Indicators (“KRI”)

KRI should be leading (forward looking) metrics to give early warning to identify potential events that may harm the continuity of major or critical business activities.

KRI should be linked to risk appetite and effective at measuring or indicating changes in the actual risk level and cover performance, economic and trend metrics. KRI are normally sourced from existing key MI (where possible) and include:

- Stress indicators monitoring any significant rise or diversion of resources;
- Metrics linked to conduct/customer outcomes;
- Causal indicators monitoring drivers of risks in view of business objectives; and
- Exposure indicators quantifying and tracking significant changes in the business environment and its exposure to critical stakeholders or critical resources (including capital).

Good KRI characteristics

- Compiled on a consistent basis, ideally from a system or ledger, to enable trend and patterns to be identified over time;
- Relevant and proportionate to the risk in question and focuses on outcomes rather than process;
- Timely and available without delay to enable appropriate action to be identified and undertaken where required; and
- Accurate and reliable, both in qualitative and quantitative content.

Risk Events

A risk event is defined as the 'risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'. This means that economic losses, reputational impacts, or control deficiencies (near miss) in a wide range of processes and business areas can give rise to risk events. Typically, a risk event can divert resources, result in a complaint, dispute or litigation, or increase reputational risk through external notifications.

- The Risk function is informed of any potentially 'Medium', 'High' or 'Very High' risk events as soon as possible, ideally within 2 working days but no later than 10 working days of first discovery and updated with relevant information at agreed intervals.

Why?

- Reduce the likelihood and/or impact of future events;
- Monitor and deliver fair customer outcomes;
- Have a centralised response that eliminates duplication of effort;
- Identify trends; and
- Understand control effectiveness.

TRAVELERS

Risk Assessment Methods: Risk Impact

Impact	Profit	Regulators, Industry or Legal Body	Reputation with Customers & Partners	People	Infrastructure
1 Very Low	<250k	• Minor *non-public* criticism of the insurance *industry* by a regulator or other industry/legal body. • Minor non-public feedback by a regulator or other industry/legal body.	• No customers at risk. • No impact on attractiveness for business partners. • Low level local or special media awareness of *industry* (including social media).	• No impact on motivation &/or trust &/or development of employees. • No impact on recruitment or attraction of talent. • No impact on employee retention, turnover or absence. • No impact on the wellbeing or health & safety of employees &/or others that the company has a duty of care to.	• Impact on less than 5 users or devices. • Tier 2 systems or minor hardware issues. • Insignificant impact to business.
2 Low	>=250k < 5m	• Warning or strong *non-public* criticism of the insurance *industry* by a regulator or industry / legal body. • *Non-public* mandatory actions by a regulator in the form of verbal feedback or a letter.	• Customers become aware of problem, a small number of low revenue existing / new customers are at risk. • Marginal impact on attractiveness for business partners. • Regional or specialist media attention of the i*ndustry*. • Multiple adverse web stories of the *industry* (including social media).	• Impact on motivation &/or trust &/or development of isolated groups of employees. • Isolated impact on recruitment or attraction of talent. • Isolated impact on turnover &/or retention &/or absence of employees. • Isolated impact on the wellbeing or health & safety of employees &/or others that the company has a duty of care to.	• Tier 2 systems or hardware availability interrupted for up to 10 users for a period of 5 - 24 hours. • Business impact is negligible.
3 Medium	>=5m < 15m	• *Public* warning or criticism of the *industry* (or a number of firms) by an industry or legal body. • Employees formally interviewed as part of a legal/ regulatory investigation. Potentially followed by a written warning.	• Significant unplanned lapses / loss of targeted new customers / impact on prospective revenue. • Some impact on attractiveness for business partners. • Long / short term media awareness confined to the insurance press. • Topic related impact on sensitive customers &/or sensitive business partners.	• Strong impact on motivation &/or trust &/or development of some key employees. • Material impact on recruitment or attraction of talent. • Material impact on turnover &/or retention &/or absence for small groups of employees. • Material negative impact on the wellbeing or health & safety of employees &/or others that the company has a duty of care to.	• Core (Tier 1) system or infrastructure offline for 5 to 24 hours for multiple users. • A major process is interrupted for up to 3 days &/or a near miss is identified in a critical business period. • IT major incident process invoked. • Overall business impact is significant.
4 High	>=15m < 25m	• *Public* warning or criticism by an industry or legal body. • Skilled Persons review or equivalent requirement from a regulator. • Notice of litigation/prosecution. • Out of court settlement(s). • Government scrutiny.	• Large number of lapses or large losses of targeted new customers. • Major loss of attractiveness for business partners. • Impact on trust in financial strength, loss in trustworthiness. • Challenge on brand &/or integrity. • Media awareness (cover / lead stories) or awareness of the company in the mainstream press. • Challenge to the trust of the Executive. • Adverse company specific topics are spreading on social media.	• Serious challenge to motivation &/or trust &/or development of significant numbers of mid management & employees. • Major impact on recruitment or attraction of talent. • Major impact on turnover &/or retention &/or absence for large groups of employees. • Major impact on the wellbeing or health & safety for large groups of employees &/or others that the company has a duty of care to.	• Core (Tier 1) system offline or major process interrupted for more than 24 hours. • Impacts the majority of employees. • IT major incident process invoked. • Material business impact. • Partial Disaster Recovery invoked.
5 Very High	>=25m	• Enforcement action (entity or individual) including fine & public censure from a regulator. • Withdrawal of membership or trading license. • Legal prosecution. • Government action.	• Very large number of lapses of top 20 accounts or huge loss of targeted new customers. • The Company becomes very unattractive for most important business partners. • Loss of trust in financial strength. • Long term media awareness (cover stories & headlines) or multiple mainstream publications or TV exposure. • Huge loss of “Trust” in the Company & its products across all important customer groups. • Challenge on the trust of the Board. • Adverse company specific social media trending/viral coverage.	• Huge loss in motivation &/or trust by mid-management & employees in the Executive. • Critical impact on recruitment / attraction of talent. • Critical impact on turnover / retention / absence of employees. • Critical impact on the wellbeing or health & safety of employees &/or others that the company has a duty of care to.	• Multiple core/critical (Tier 1) systems offline. • Major business process interrupted for more than 3 days. • Major business (first line of defence) process is interrupted for more than 12 hours. • IT major incident & full Disaster Recovery processes invoked.

Risk Assessment Methods

Risk Register Likelihood

Likelihood	Description		Frequency
1 **Rare**	A loss scenario as a result of the risk is estimated to occur only in *exceptional* circumstances	< 10 %	Less than once every 10 years
2 **Unlikely**	A loss scenario as a result of the risk is estimated to occur *relatively infrequently*	10 - 20 %	Once every 5 to 10 years
3 **Possible**	A loss scenario as a result of the risk is estimated to occur *occasionally*	20 - 50 %	Once every 2 to 5 years
4 **Likely**	A loss scenario as a result of the risk is estimated to occur *regularly*	50 - 90 %	Every 1 to 2 years
5 **Almost Certain**	A loss scenario as a result of the risk is estimated to occur *frequently*	> 90 %	About once a year

Risk Register Internal Controls

Rating	Description
1 **Poor**	No risk mitigation activities are in place i.e., no controls operate or exist.
2 **Unsuitable**	Controls are unreliable & not continuously applied. Frequently they did not operate as intended or there have been frequent failures. They are poorly designed, inefficient & unable to automatically adjust to changes.
3 **Fair**	Controls are in place, effective & continuously applied. There may be isolated instances of the control not operating as planned or failure, controls may not be well designed, may not be efficient nor able to automatically adjust to changes.
4 **Good**	Controls are effective, continuously applied & well designed with some extremely limited instances of not operating as planned or failure. Some may be slightly inefficient nor able to automatically adjust to changes.
5 **Excellent**	Controls are effective, continuously applied & very well designed with no instances of not operating as planned or failure. All controls are fully automated, efficient & able to automatically adjust to changes.

TRAVELERS

Emerging Risks

Defined as an 'issue, risk or trend that has potential implications (positive or negative) and could materially impact the company from a book of business, underwriting, claims, financial, regulatory, reputational or political perspective'.

- Emerging risks, issues or trends that are not tracked on the risk register taxonomy (i.e. not within a 12-month time horizon) but could impact, or pose a potential threat to, the business over the medium to long term.
- The early identification of emerging risks, trends or issues enables management actions to be prioritised and resourced to enhance business resilience.
- Emerging risks may change or modify known risks (documented in the risk register), create new risks/risk drivers, or present opportunity to the business to reduce, mitigate, accept and transfer risks.

How?

- Scan the horizon for future risks on a continuous basis to identify, raise and assess emerging risks.
- All employees also have the ability to raise emerging risks. This internal crowdsourcing method seeks to provide an early indication of what might lie beyond the horizon and could become relevant to the business going forward.

Stress & Scenario Testing

Stress and scenario testing is an important forward-looking risk management tool. It forms a key part of the RMF as it is used to develop robust and integrated business, capital and risk plans and demonstrates the strong linkages between these core elements of the strategy. It also assists in discussions of low probability events or events that have not occurred in the recent past, or at all. Such risks often receive low assessments in the Risk Register, so they can be introduced through stress and scenario testing.

- Capital Model
- Risk Register
- Emerging Risk Index
- Risk Events and External Benchmarking
- Regulatory Releases
- Roundtable
- Group

- Multi Year
- P&L/Capital impact
- Regulatory, Industry and Legal Body impact
- Customer and Partner impact
- People impact
- Infrastructure impact

- Inter-relationships
- Secondary impacts
- Aggregation and Interdependency
- Capability Analysis
- Gauge Responses
- Return Period
- Mitigation

- Potential Management Actions
- Review / Enhance Processes
- Model / Methodology Development
- Validation items

TRAVELERS

Linking Risk Management to Company Insurances

- A company must have appropriate insurances in place that reflect its risk profile. Risk teams are accountable for providing oversight of their firm.
- Insurance does not prevent something from occurring. If something unexpected does happen insurance means a company won't have to fund the full costs of the loss.
- Not all risk can be covered by insurance as there are many risks that do not have a direct financial impact and alternative risk management strategies would be required.
- Risk-based decisions can also be made not to accept a risk, where a cost benefit assessment determine insurance is not the best option i.e. accept / mitigate.

Key Factors for a Responsible Body to consider include:

- Ensure the company considers all insurable risks and is insured appropriately.
- Determine the appropriate level of insurance based on consideration of the company's risk profile for the next 12 months.
- Ensure that a current register of insurance and indemnities is maintained and linked to the risk management system.
- Ensure that the financial impacts of any indemnities have been adequately assessed and align with the company's risk appetite.
- Ensure risk event data, including near misses, is provided to the Risk function / Insurer.

TRAVELERS

Summary Risk Profiling

Passion for Order & Evidence

Every future company endeavour will rely on the readiness of the risk management system. Structure and terminology is fundamental for credible data sources that drive rational forecasts and valid forensic analysis of incidents/events.

Decision Making Based on Facts & Specialist Assessments

Relationships with the subject matter experts and data sources to understand assumptions and behaviour.

Continuous Improvement

The business profile is never static and data models might only come slightly close to the optimal results. The real world is very difficult to account for and figuring out every situation is virtually impossible.
Continuously develop and tailor risk profiling to meet evolving business requirements.

Disclaimer

- This presentation is intended for discussion purposes only and does not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenter individually and, are not the opinion or position of any company, governing body, professional body, consultancy or software/database consortium or vendor.
- This presentation summarises a hypothetical risk framework linked to UK financial services regulatory reporting and does not imply endorsement by any company, governing body, professional body, consultancy or software/database consortium or vendor.
- The presenter does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

TRAVELERS

Thank You