Protecting and Creating Value through Operational Risk Management

24th Annual Insurance Issues Conference

Monday, November 30, 2015

Agenda

1. Introduction
2. Definition and classification
3. Quantification
4. Benefits
5. Industry practices
6. Call for Action

Operational Risk in the Financial Services sector

Early 2000

- Comprehensive Op. Risk policy
- Formal framework for ORM
- Improve Op. Risk understanding & ownership
- Practical tools to identify and manage Op. Risk
- Enterprise-wide RCSA program
- Automated tools and systems readiness
- Principles for ORM methodologies including loss data collection and capital models
- Risk management integration initiatives

2005-2009

- Further evolution of Op. Risk Policy Framework
- AMA objectives
- Data Challenge: Use output of operational risk quantification to drive key risk management initiatives
- Organization structure – "Federated Model"
  - ORM Corporate Team
  - Risk Team
  - Partners
- ORM staff training and development

2009-current

- Strengthened ORM mandate and stature
- ORM into risk appetite statements linked to senior management performance/evaluation
- Enhanced scenarios analysis (stress testing)
- EC models / AMA - embed EC in business decisions
- Realignment of governance model targeted at increased transparency
- Enhanced reporting
- Standardized risk taxonomy

Proposed Updates

- Issues identified with design and effectiveness of the ORM program (mechanisms, internal controls, and firm-wide monitoring of Op. risks)
- Enhancements required:
  - Risk taxonomy
  - Risk appetite
  - Loss data collection
  - KRIs
  - RCSA
  - Processes mapping (to identify key controls)
  - Scenario analysis
  - Change Management
  - Review of policies
  - Audit findings
  - 3 lines of defense

Some Examples of Common, But Usually Unreported Operational Risk Events

LOSS CATEGORY	DESCRIPTION
Theft and Fraud	• Fraudulent claims – fabricated events by fraud rings; exaggerated claims. • Unreported deaths for annuities and pensions. • Jumbo commissions on fraudulent life policies.
Unauthorised Activity	• Internal collusion with external claims or other service providers.
Suitability, Disclosure and Fiduciary	• Failure to comply with training and sales practices requirements by sales force. • Failure to provide adequate selection and oversight of sales force.
Clients, Products and Business Practices	• Failure to apply underwriting or claims settlement standards. • Over-rides of underwriting or claims settlement standards.
Clients, Products and Business Practices	• Errors in product design or pricing.
System Failures	• Interface errors between billing and receivable systems. • System configuration errors affecting complex computations. • Loss of data.

Operational Risk – Regulatory Guidance

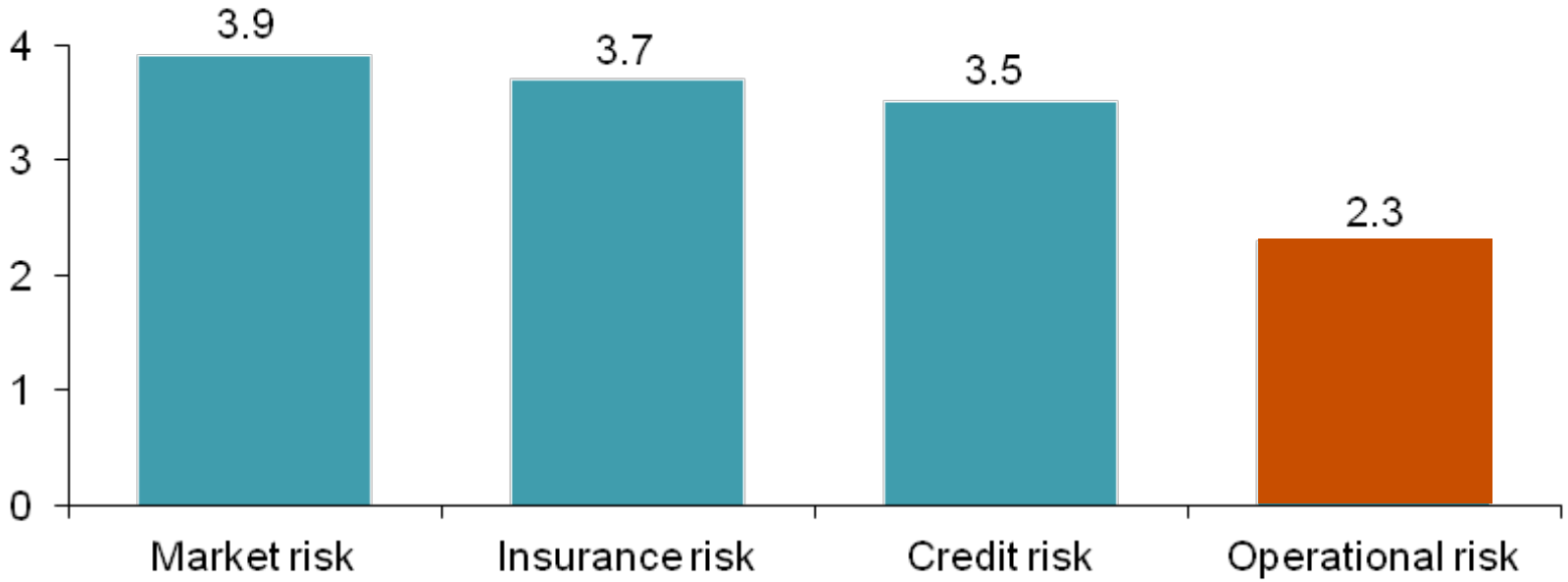
DATE	SOURCE	PUBLICATION
Superceded	OSFI	Sound business and financial practices framework for life insurers. Proposed but not introduced for P&C insurance
May 2006	OSFI	Corporate Governance at TSA (The Standardized Approach) & AMA (Advanced Measurement Approach) Institutions
Ongoing	Solvency II	Models for measuring capital required, including specific amounts for operational risk
June 2011	BCBS	Principles for the Sound Management of Operational Risk
June 2011	BCBS	Operational Risk - Supervisory Guidelines for the Advanced Measurement Approaches
August 2011	OSFI	Memo to Banks referencing BCBS - Principles for the Sound Management of Operational Risk: *"the principles outlined in the 2011 paper establish **sound practices** that are **relevant to all** deposit-taking institutions, and expects institutions to take account of the nature, size, complexity and risk profile of their activities when assessing their practices against the updated principles in the Principles paper in the course of normal compliance reviews. Institutions should develop a **plan to remedy any deficiencies** that come to light during their assessments."*
September 2012	OSFI	OSFI issued Life Insurance Regulatory Framework, indicating that future life insurance capital requirements will be introduced that include specific margins for operational risk.
Summer 2015	OSFI	Draft guideline issued for federal financial institutions

Operational risk implementation challenges

	Challenges	Responses
Effective Operational Risk Taxonomy	• Missing or unclear risk definitions • Multiple and overlapping definitions • Non-compliance with regulatory standards	• Business Analysis / peer comparison • Tied to Risk Appetite – NOT loss events • Business development of risks
Internal & external loss data collection/analysis	• Inadequate, missing, inconsistent loss data • Calibration / extrapolation of external data • Inappropriate data-related assumptions	• Structured data gather for losses / **near-misses** gathering process • Templates to gather internal data
Operational Risk Modelling	• Data-poor environment • Costly modelling techniques • Confidence in adequacy of modelling	• Leveraging data sharing arrangements • Cost-benefit analysis of advanced modelling • Use of commensurate modelling techniques
KPI's and KRI's	• Non-alignment with institution's risk profile • Computational challenges • Unable to contribute to decision making	• Clear articulation of risk profile • Non-conflicting & forward-looking KPIs/KRIs • Engagement with Senior Management
RCSA Program	• Incomplete coverage of RCSA • RCSA not meeting institution's needs • Inconclusive results due to subjective scoring	• Development of RCSA Framework • Enterprise-wise RCSA / ORSA • Backed by interviews with SMEs

Quantification – Effectiveness of Risk Modelling

Operational risk is clearly an area where companies are still not satisfied with the effectiveness of current modelling techniques …



Source: KPMG International Economic Capital Survey, 2011-12

Monitoring Operational Risk Indicators

Purpose of Key Risk Indicators

- Factors that may provide early warning signals on systems, processes, products, people and the broader environment
- Scorecard format facilitates easy identification of areas potentially posing increased levels of risk
- Can be structured to provide forward looking and historic based metrics
- Relies upon observable data as opposed to estimates of future activities (as is normally used in risk assessments) to produce a timely representation of the level of risk
- When combined with risk assessment and loss data gathering results, the cumulative information can provide a comprehensive profile of operational risk

Application of Key Risk Indicators

- Risk areas to be monitored selected and relevant KRIs identified. (Identification of KRIs with close correlation to actual exposure can only be determined over time)
- Initially, normally a generic series of indicators developed that are applicable across the organization
- Thresholds for each KRI developed to allow priority areas to be identified
- Thresholds can be set at business line and organizational level
- Comparison to loss data increases transparency
- The collection and collation of KRIs will require the design and implementation of supporting processes

Monitoring Operational Risk Indicators
Examples

Some Examples of insurance KRIs

- New business application – acceptance and rejection rates; mix of standard vs. substandard risks submitted and accepted
- Claims adjuster statistics – number of claims handled, average costs
- Open claims inventory/backlog/new claims opened statistics
- Claims experience vs. expected
- Reopened claims files
- Customer complaint statistics

Effectiveness of Key Risk Indicators

- Distinction between **predictive**, **preventive** and detective **indicators** – you need all, but...
- **Recent example** – public scandal over retiree benefits fraud at Long Island Railroad; for several years, a very high percentage of retirees retired, often early, claiming disability benefits – long after these statistics were observed, losses had accumulated to $1B

Operational Risk and Risk Appetite

Example risk appetite statements:

	Risk appetite statement	Risk tolerance limit	Key risk indicators	Business unit level
Operational	**Outsourcing** – Outsourced processes will be subject to outsourcing best practices such as those set out in OSFI Outsourcing Guideline B-10.	Compliance with outsourcer service level agreements is to be monitored and any gaps remediated on a timely basis.	• Trending in reported exceptions • Service level metrics vs. SLA standards	KRIs can be the same at BU level
Operational	**IT security** – The company will mitigate information security risks to achieve a high level of protection of customer personal information, and of proprietary information.	(commonly n/a, a "zero tolerance" item)	• Attempted penetrations, security breaches	KRIs can be the same at BU level

Operational Risk practices seen in 2014 ORSAs

Source: "*Own Risk and Solvency Assessment: Canadian current state observations*" (KPMG in Canada, 2014)

- Risk appetite statements generally need some work, including for op risk
  - More quantitative measures/limits
  - For "zero tolerance" statements, relate to how you would monitor compliance
- Op risk measures tended to default to regulatory standard formula – some more sophisticated approaches such as scenario analysis observed
- Operational risk understanding and data is generally minimal; framework should include elements of:
  - Internal loss data collection
  - Key Risk Indicators as a monitoring tool
  - Operational risk taxonomy
  - Business environment internal control factors
  - Risk and control self assessments

Operational Risk

Definition and Classification

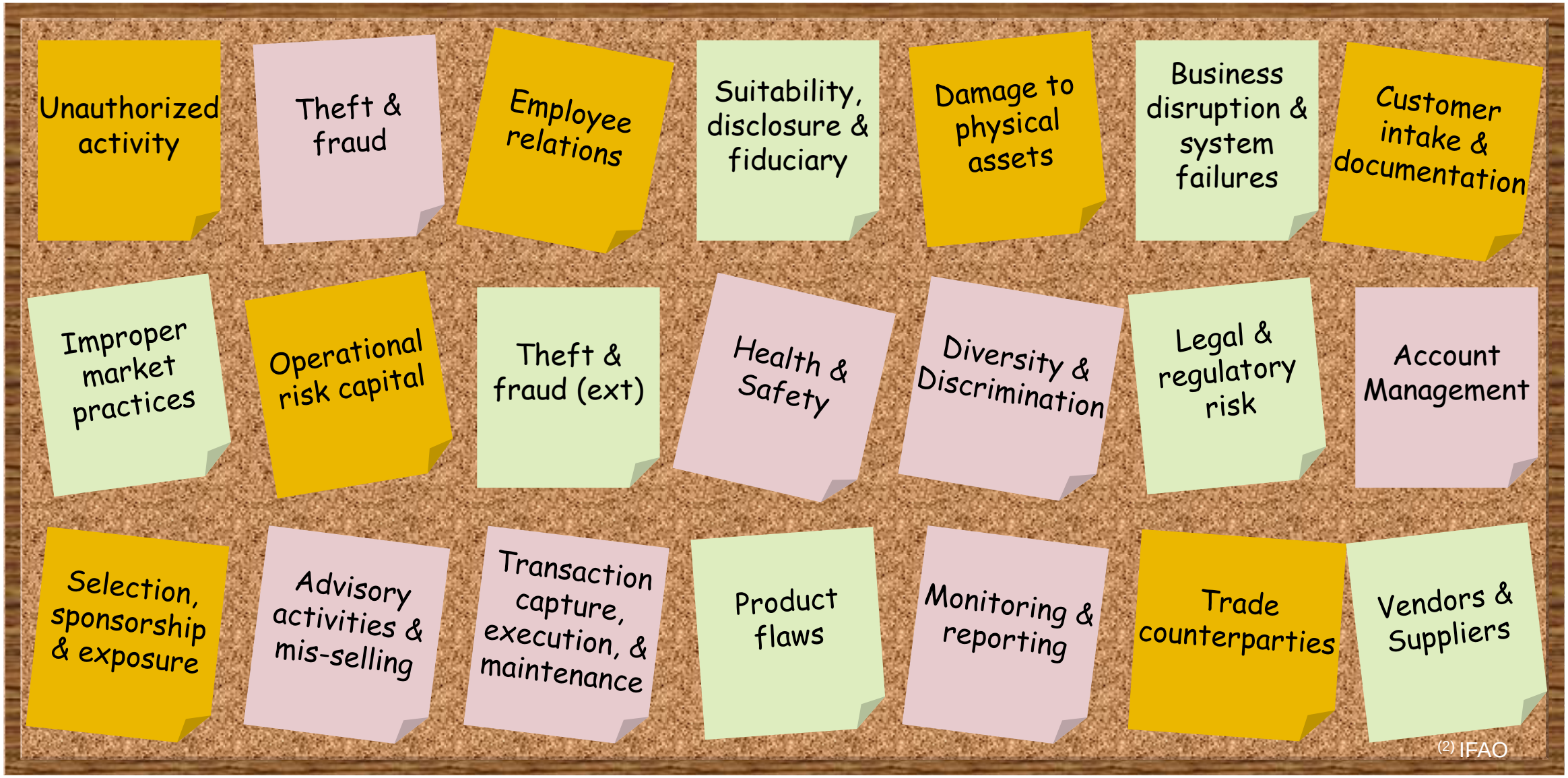
Integrated Risk Management

COMPLETENESS OF RISK COVERAGE

Operational risk is defined as the risk resulting from people, inadequate or failed internal processes and systems, or from external events [1]

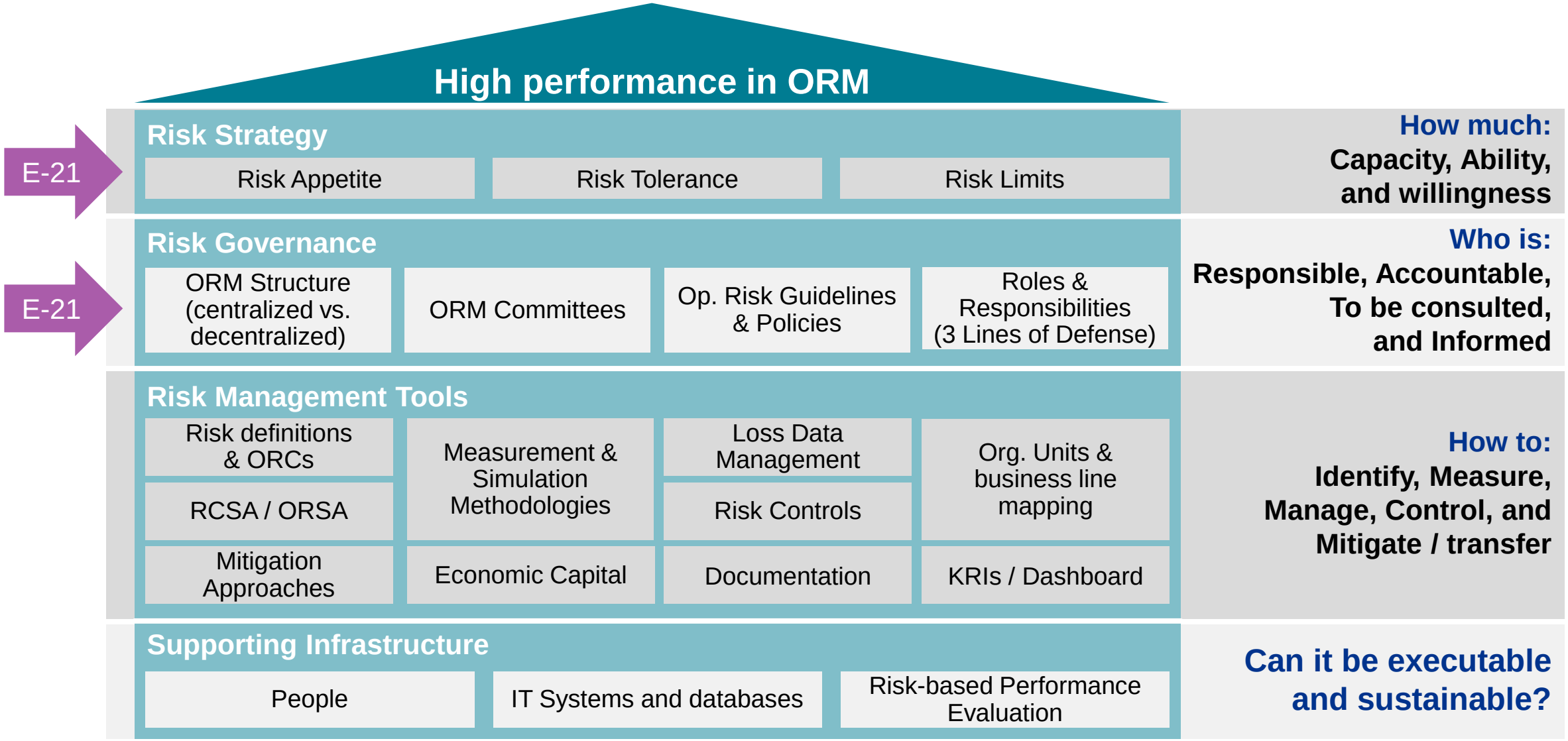
[1] OSFI Draft E-21

Operational Risk Taxonomy [2]



[2] IFAO

Operational Risk Management Framework



Operational Risk

Quantification

Operational Risk in MCT

$$\text{Operational Risk Margin} = Min\left\{\begin{array}{l} 30\%CR_0, \\ \left(8.5\%CR_0 + 2.5\%P_w + 1.75\%P_a + 2.5\%P_c + 2.5\%P_\Delta\right) \\ +Max(0.75\%P_{aig}, 0.75\%P_{cig}) \end{array}\right\}$$

= total capital required for the reporting period, before operational risk margin and diversification credit

= direct premiums written in the past 12 months

= premiums assumed in the past 12 months

= premiums ceded in the past 12 months

= growth in premiums in the past 12 months (premium growth charge)

= assumed premiums written in the past 12 months arising from intra-group pooling arrangements

= ceded premiums written in the past 12 months arising from intra-group pooling arrangements

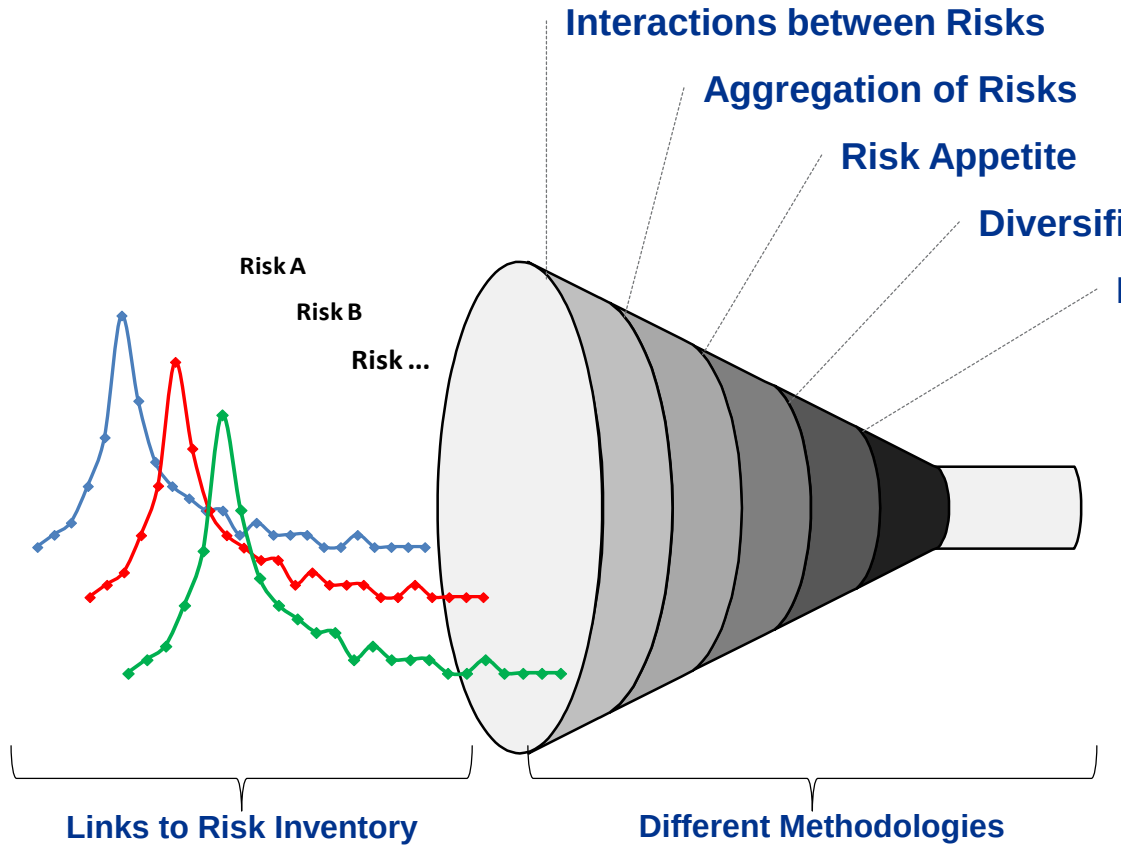
Operational Risk In MCCSR

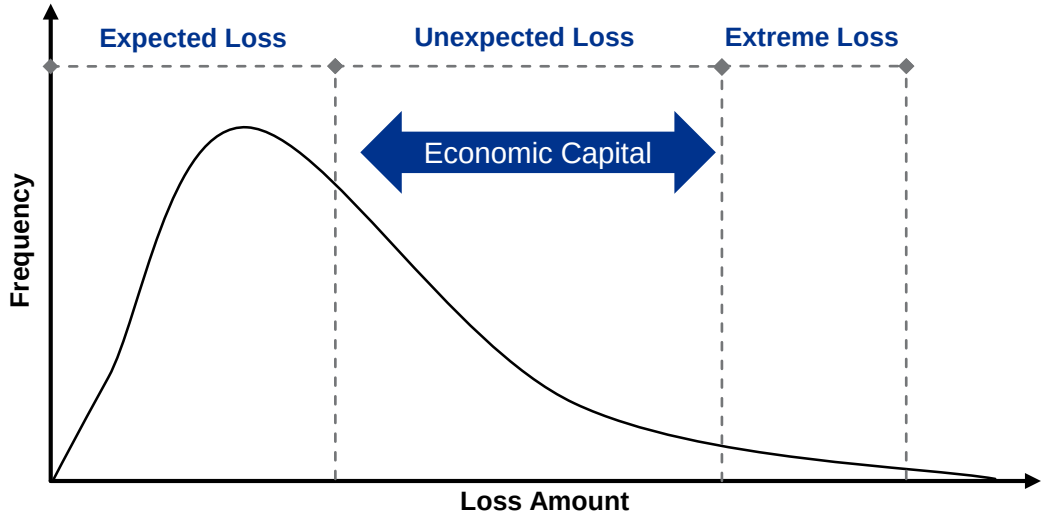
With respect to the Total Ratio, if considering only the risks where calculations are specified, a minimum Total Ratio of 100% may be considered acceptable. However, **life insurers** are exposed to **more risks** than those for which calculations are specified

Consequently, the minimum Total Ratio for **life insurers** is set at **120%** rather than **100%** to cover operational risks that are not explicitly measured, but which form part of the minimum requirement under MCCSR/TAAM

Economic Capital

Economic Capital is defined as sufficient surplus that would be needed to cover potential losses at a given risk tolerance, over a specified time horizon, based on a probabilistic assessment of potential future losses





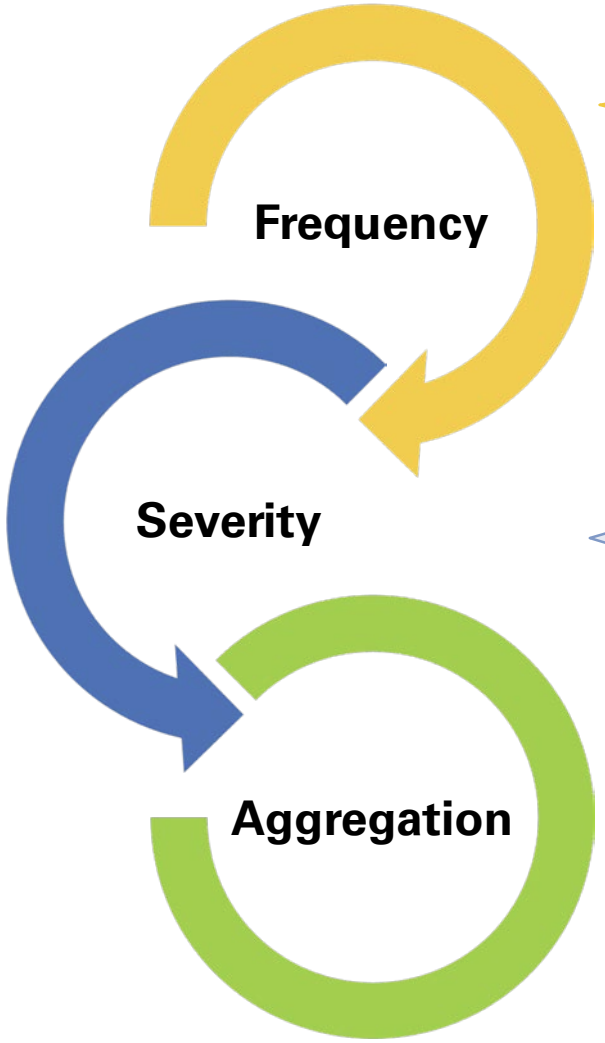
Scenario Analysis (What If)

Operational Risk component of EC

By aggregating the scenarios allowing for correlation

- Experts & Judgment
- Number of scenarios
- Severity & Probability
- Adjustments (e.g. Historical to Actual)
- Inherent/Net Risks

Frequency-Severity Approach (Modeling)



Probability that one or more events will occur

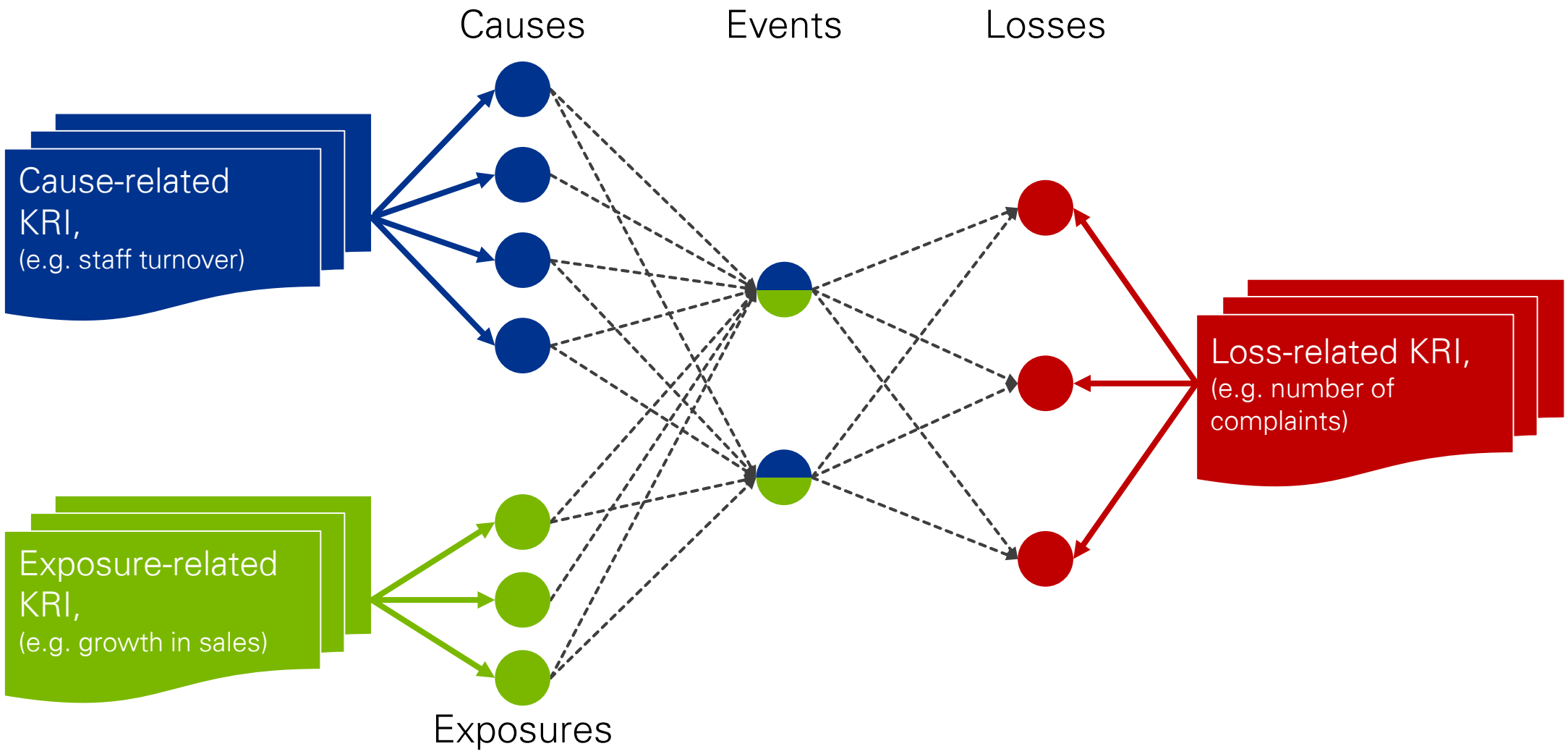
- Bernouilli
- Poisson
- Negative Binomial
- Binomial

The size of an event given its occurrence

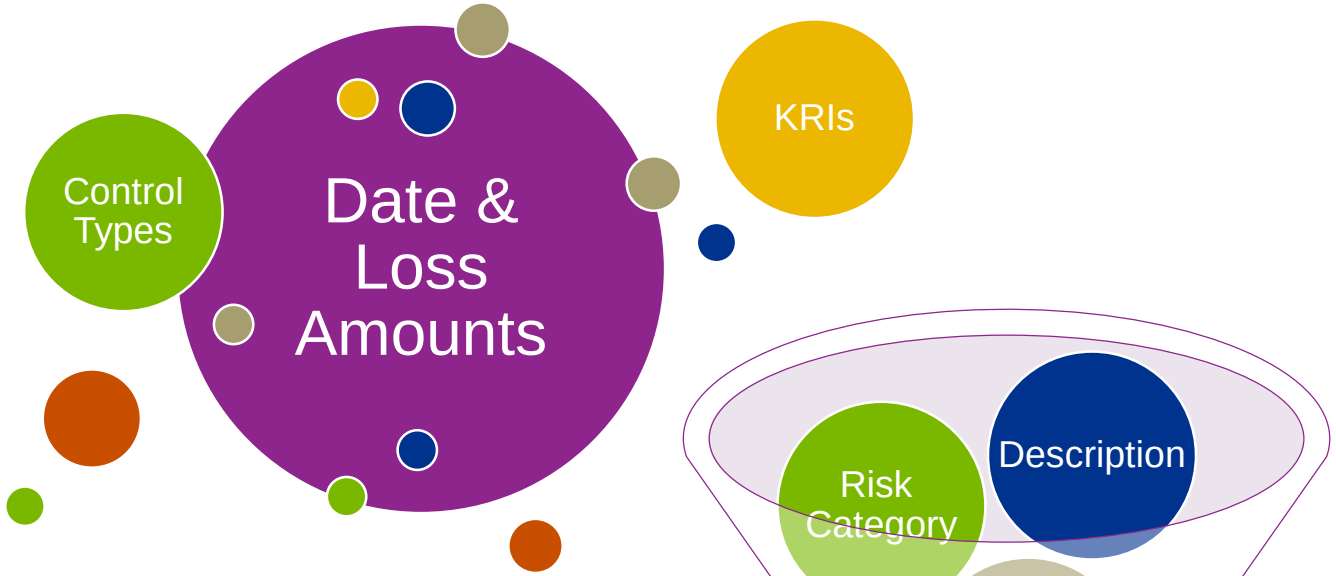
- Lognormal
- Pareto
- Gamma
- Weibull
- Exponential
- Beta
- Generalized Pareto

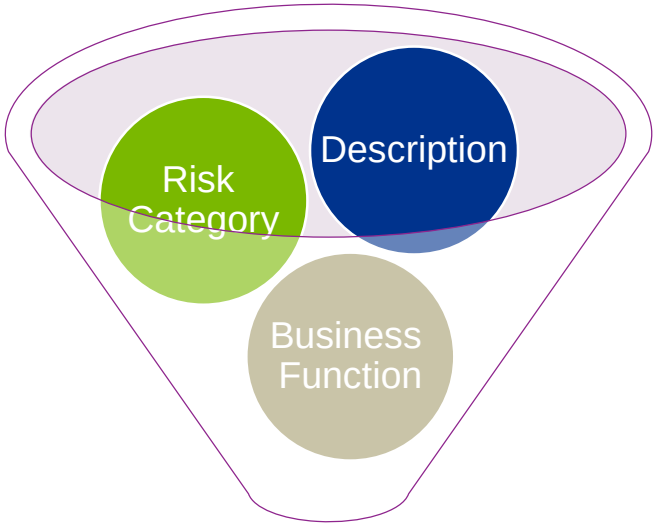
Correlation
Ripple-effect

Causal Modeling and Bayesian Techniques



Sources of Operational Risk Loss Data





E-21

ORIC, ORX, AON OpBase, Fitch FIRST Database

Operational Risk

Framework and Benefits

Operational Risk Appetite Statement

OSFI – Corporate Governance

Key features

- Senior management commitment and sign-off
- Documented in the form of a risk policy
- Risk policy document owned and updated by the risk manager, approved by the Board

Key Features

- Link to the firm's short-term and long-term strategic, capital and financial plans, as well as compensation programs
- Include qualitative and quantitative measures that can be aggregated and disaggregated
- Be forward-looking
- Consider normal and stressed scenarios
- Aim to be within the insurer's risk capacity (i.e., regulatory constraints)

Benefits

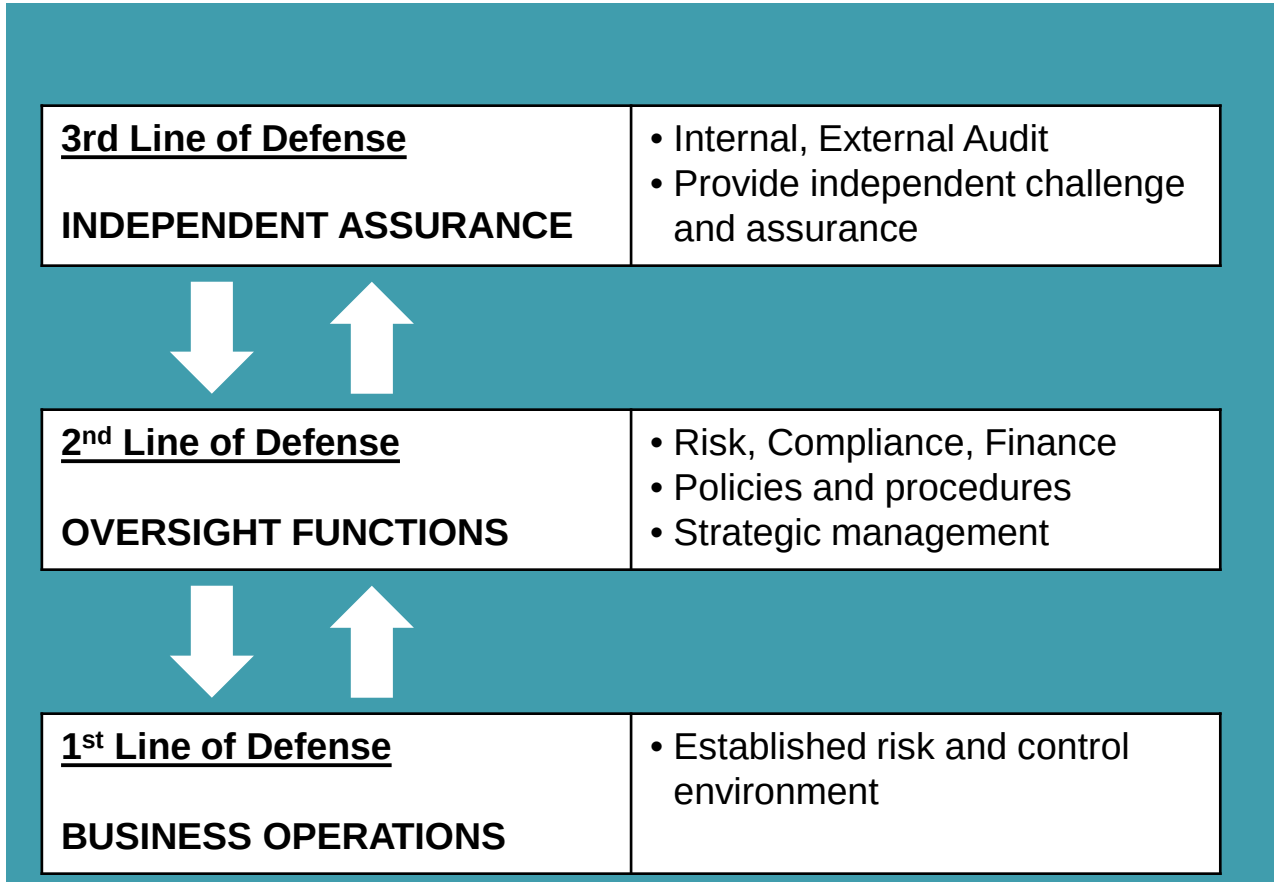
- Provide overall clarity and direction for managing risk
- Ensure relevance to the businesses
- Demonstrate senior management buy-in to risk management framework
- Provide guiding principles upon which other framework components will be based

Three Lines of Defense – An Illustration

Organizational and reporting structures for managing risk and performance measurement

Key features

- Detailed design of roles, responsibilities, key interfaces and reporting infrastructure for a selected model
- Linkages between risk management performance and your performance measurement strategy
- Alignment of HR policy to selected individual's specific responsibilities for risk management



Benefits

- Building a robust organization model for risk will ensure:
  - Clarity of roles and responsibilities of all parties involved in the risk management process
  - Interfaces are understood
  - Reporting infrastructure is defined
- Linking risk management performance to business targets and personal contracts increases overall levels of commitment to improving risk management effectiveness

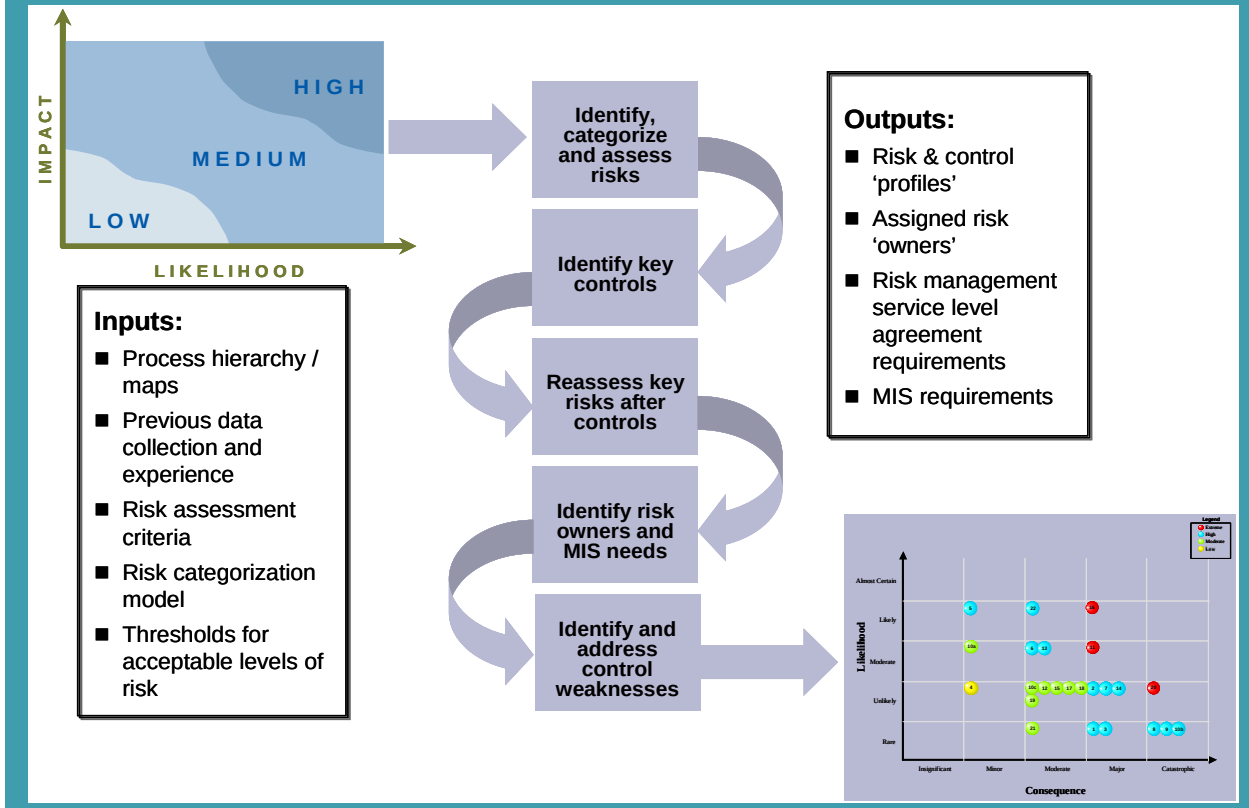
Risk Assessment and Quantification

A quantitative approach to identify potential loss events of a primarily severe nature.

Features

- Consistent method for evaluating and reporting risks and controls pre and post control
- Improves risk transparency and promotes common understanding of risks and controls
- Provides a means through which more risk sensitive and forward looking data can be derived.
- Thresholds developed to reflect the risk appetite of the organization.

Validation of results important



Benefits

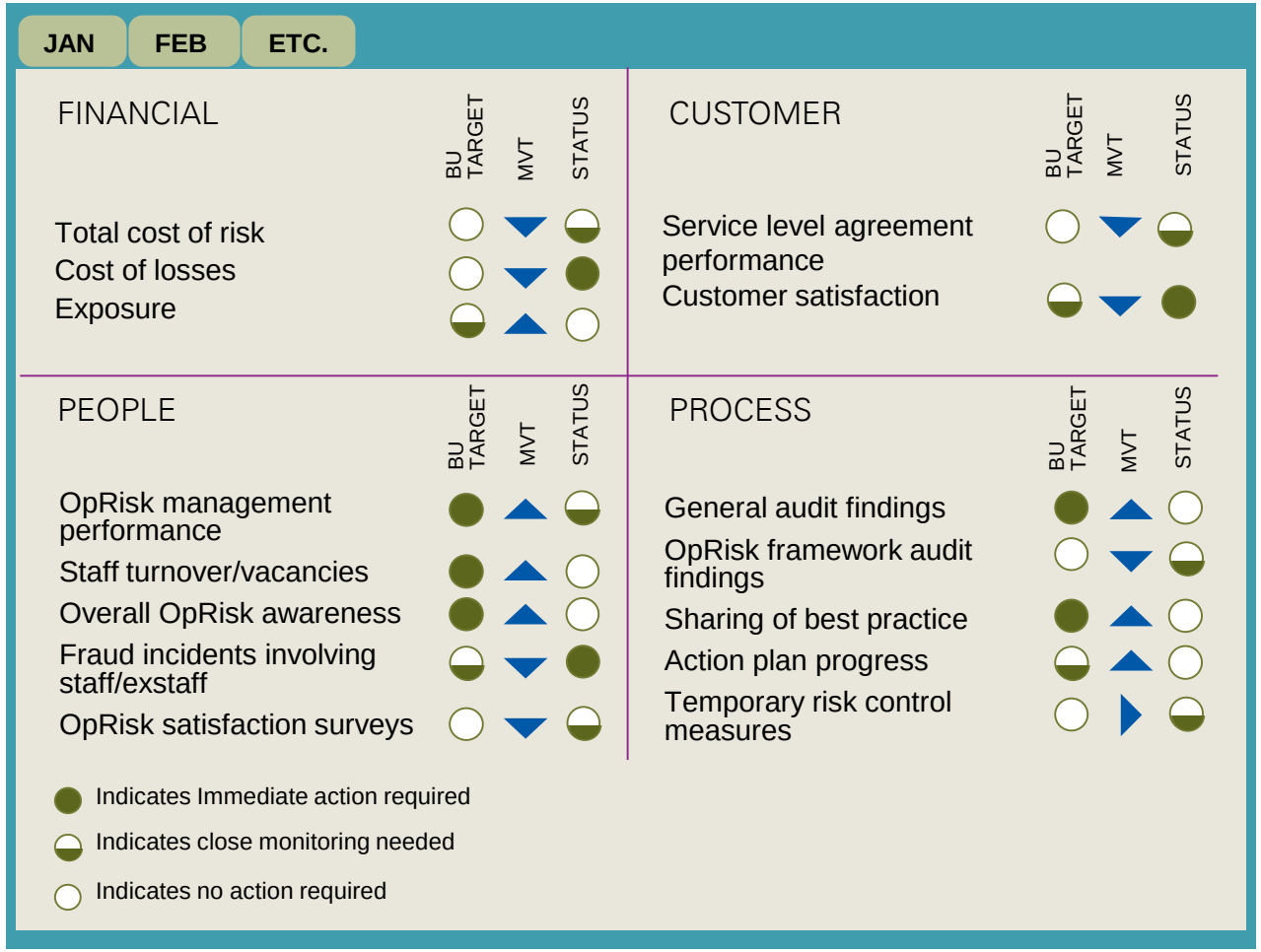
- Risk profiles and associated action plans used to monitor and ultimately reduce the level of risk within the business.
- Determines priority areas for improvement (risk and controls) enabling effective allocation of resources
- Data series can be used in more quantitative approaches to risk measurement.

Key Risk Indicators – Dashboard Reporting

Factors that may provide early warning signals on systems, processes, products, people and the broader environment

Features

- Thresholds developed to reflect the risk appetite of the organization
- Thresholds can be adjusted over time to encourage higher standards of risk management
- Can be used in quantitative and economic capital approaches to reward high standards of operational risk management



Benefits

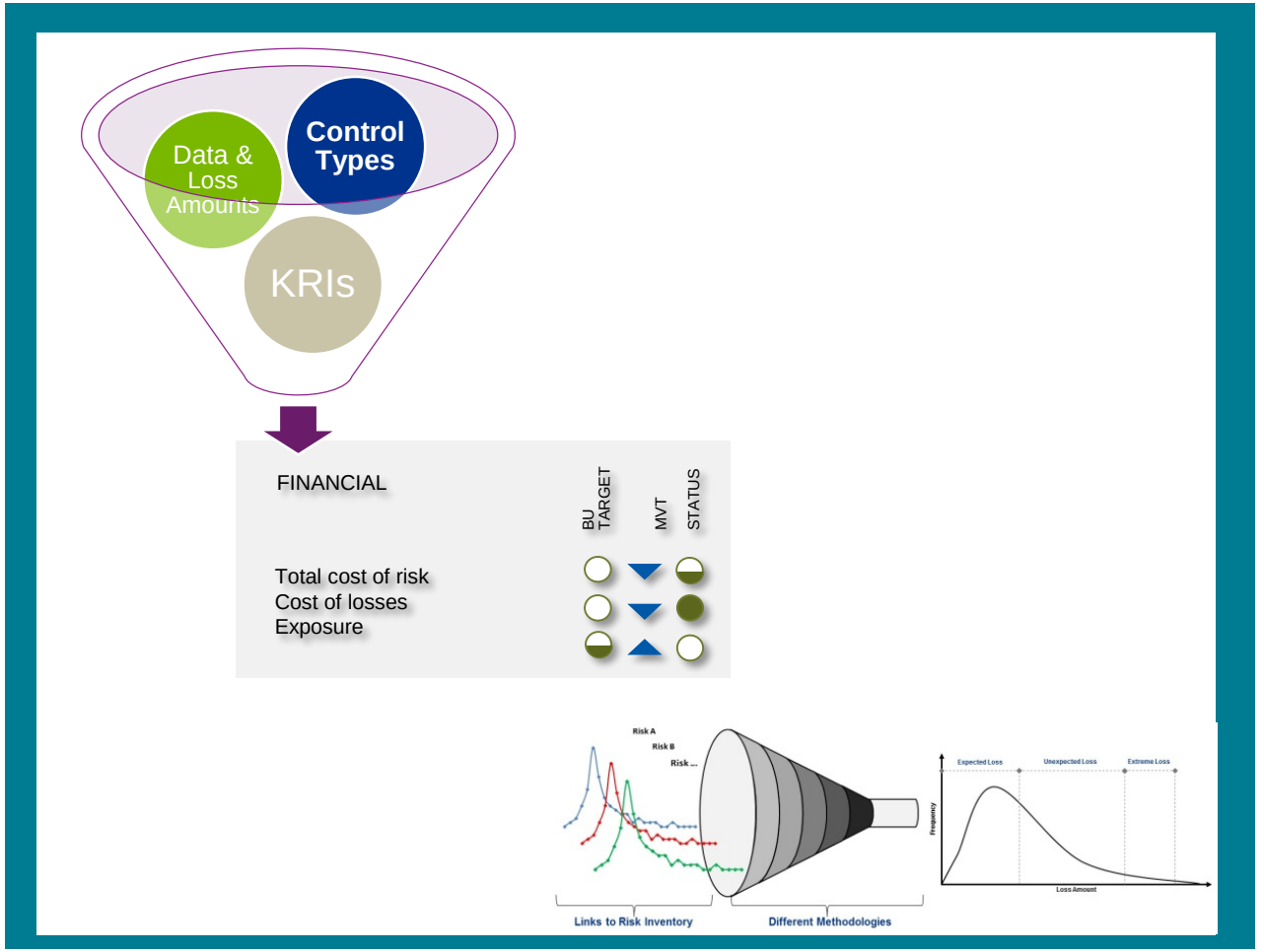
- Facilitates identification and monitoring of potential risk areas
- Encourages a pro-active approach to the management of operational risk
- Provides an accessible means of management information for executives
- Aids benchmarking activities between business lines

Data Collection

Process for collecting, evaluating, monitoring and reporting operational risk loss data, to provide an important metric in the measurement operational risk

Key features

- Highly visible process to facilitate the collection of loss information
- Process integrated into daily business activities
- Clear scope around data required
- Guidance for quantification, arrangement and weighting of data
- Pre-requisite to the development of quantification and economic capital models for operational risk

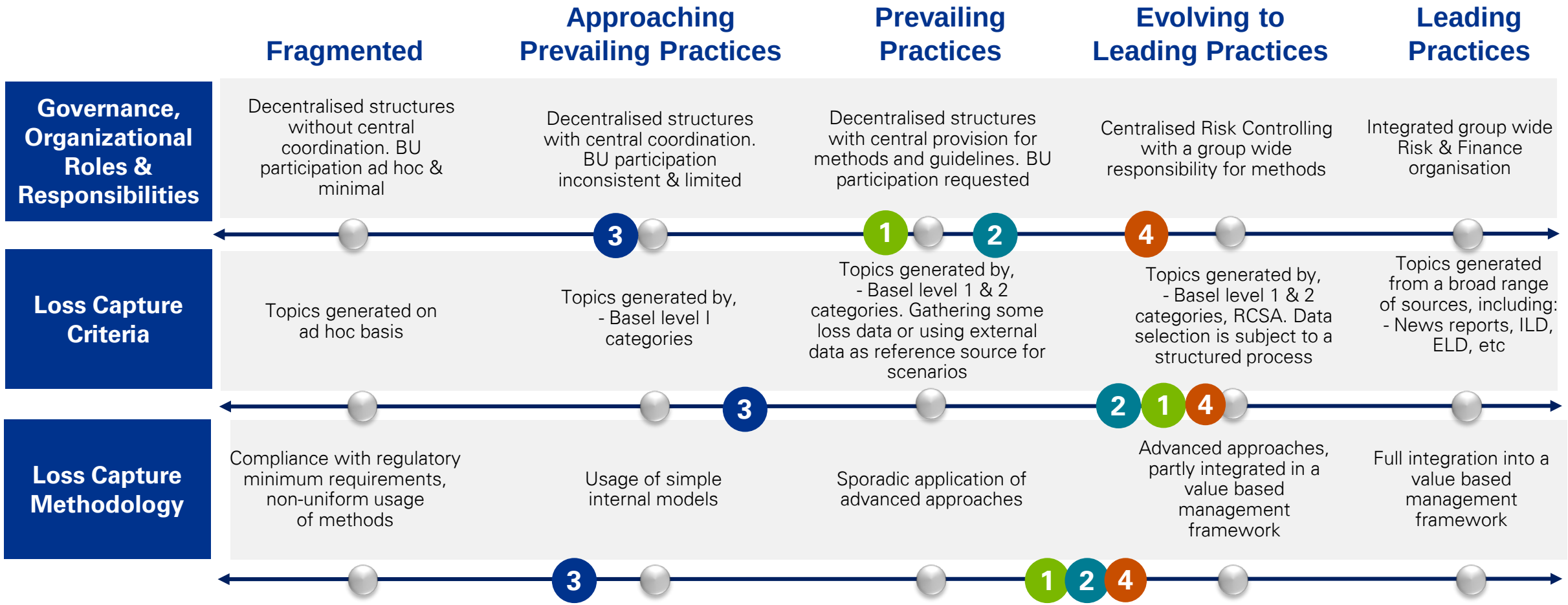


Benefits

- Contributes towards the development of a complete operational risk profile
- Provides a quantifiable and tangible metric, used to gauge the effectiveness of the framework
- Aids identification of risk ‘hot spots’ and allocation of resources to priority areas
- Raises awareness on the importance of proactively managing operational risk

Industry Practices Regarding Operational Risk

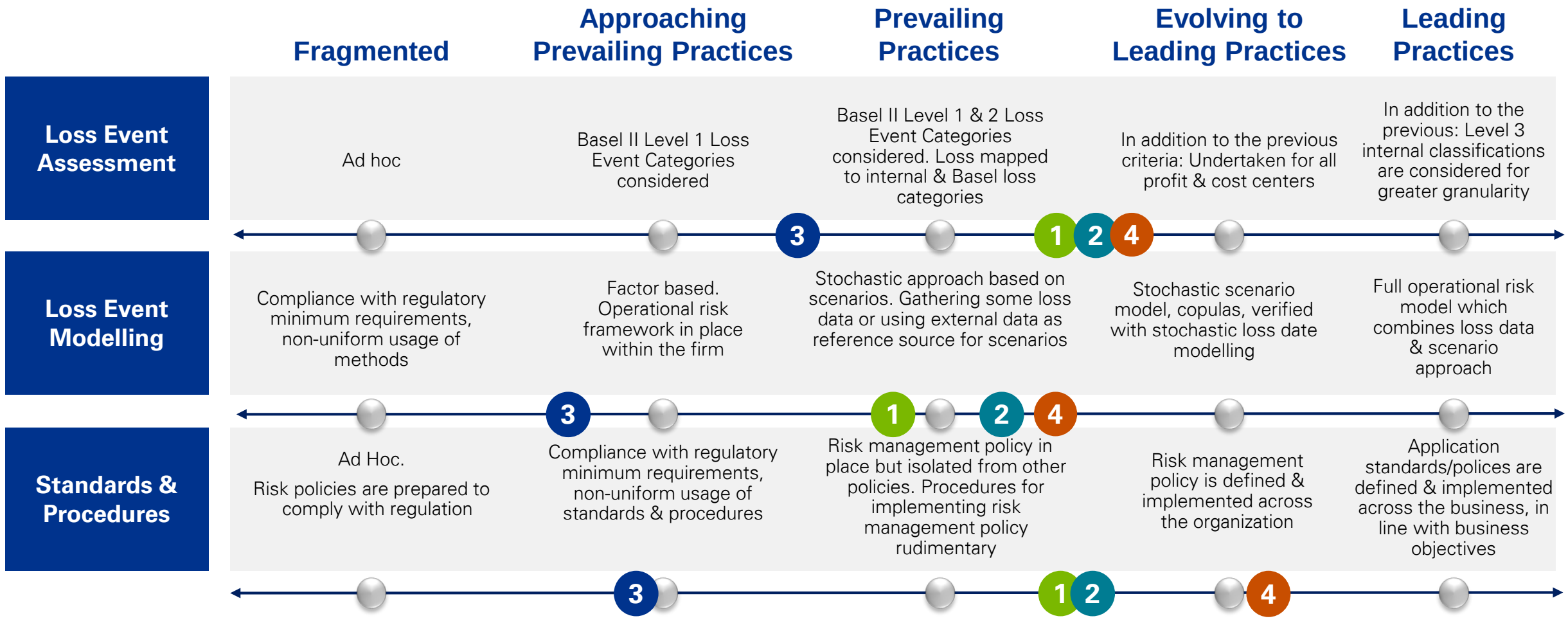
Operational Risk Maturity – 1 of 3



Benchmarking comparisons:

- 1 **Global Insurance Firms (non-US)**
- 2 **Asset Mgmt Firms**
- 3 **Global Insurance Firms (US)**
- 4 **Multinational Banking Firms**

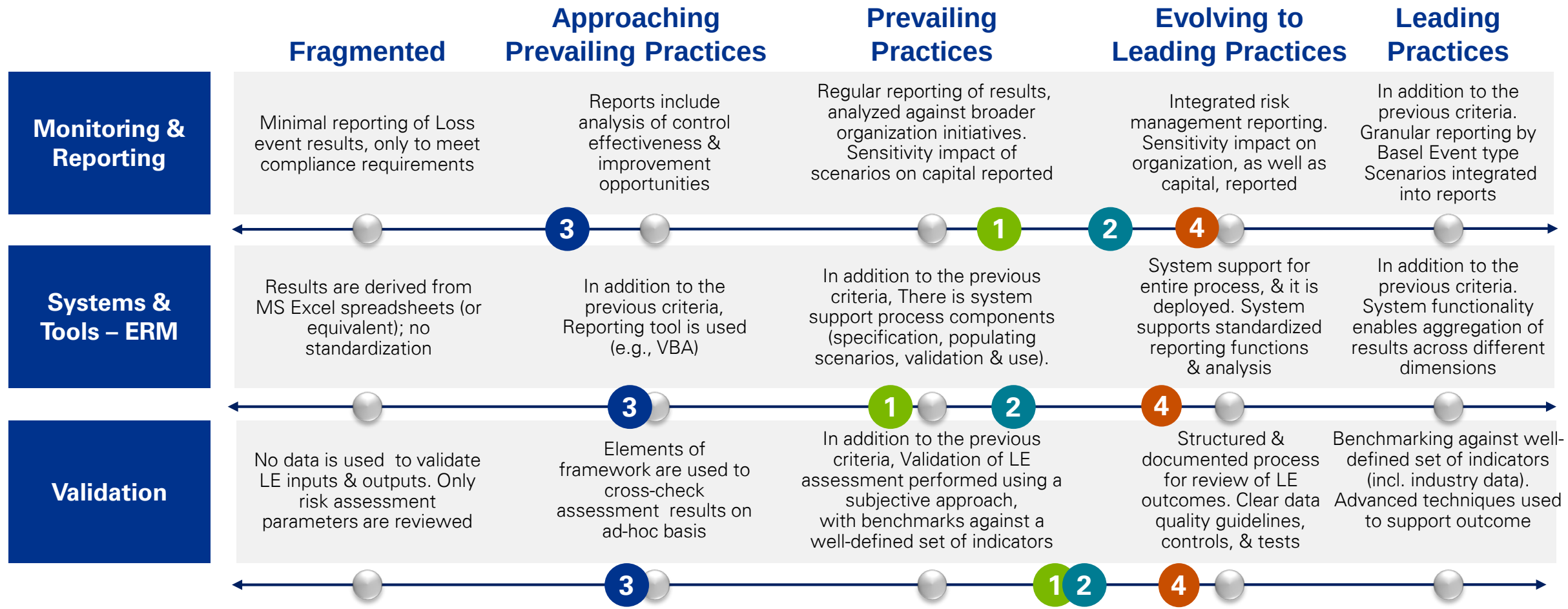
Operational Risk Maturity – 2 of 3



Benchmarking comparisons:

- 1 **Global Insurance Firms (non-US)**
- 2 **Asset Mgmt Firms**
- 3 **Global Insurance Firms (US)**
- 4 **Multinational Banking Firms**

Operational Risk Maturity – 3 of 3



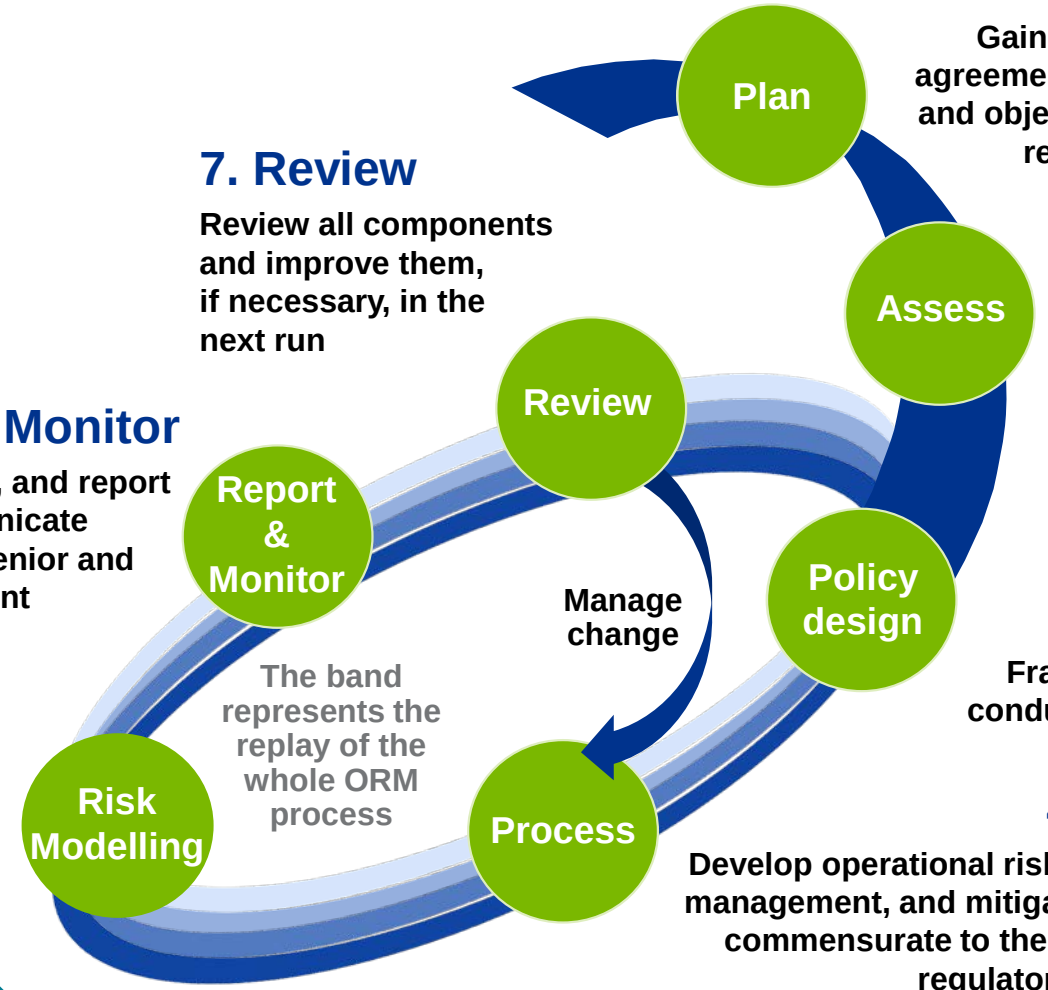
Benchmarking comparisons:

- 1 **Global Insurance Firms (non-US)**
- 2 **Asset Mgmt Firms**
- 3 **Global Insurance Firms (US)**
- 4 **Multinational Banking Firms**

Operational Risk

Call for Action

Next Steps



1. Plan

Gain an understanding and agreement regarding the scope and objectives of the proposed regulatory requirements

2. Assess

Perform a gap analysis and develop a roadmap to mitigate gaps around policy, process, people, data, and technology

3. Policy design

Design an Operational Risk Management Policy and Framework, risk taxonomy, and conduct ORSA (incl. risk appetite)

4. Process

Develop operational risk measurement, management, and mitigation processes commensurate to the risk profile and regulatory requirements

- ✓ Risk and Control Self-Assessment
- ✓ New Business, Product & Initiative Approval Process
- ✓ Incident Reporting & Investigation

5. Risk Modelling

Develop a roadmap to move from basic to more advanced measurement approaches

- ✓ Data Collection

6. Report & Monitor

Develop, monitor, and report KRIs and communicate effectively with senior and junior management

7. Review

Review all components and improve them, if necessary, in the next run

Neil Parkinson
Partner, Insurance Practice
416-777-3906
nparkinson@kpmg.ca

Alex Shipilov
Partner, Financial Risk Management
416-777-3026
ashipilov@kpmg.ca

Anh Tu Le
Senior Manager, Actuarial Services
647-777-5352
ale@kpmg.ca