OLIVER WYMAN

CAFRAL
CENTRE FOR ADVANCED FINANCIAL RESEARCH AND LEARNING
Promoted by Reserve Bank of India

OPERATIONAL RISK MANAGEMENT
PERSPECTIVES FOR SUPERVISORS

6 FEBRUARY 2013

Dr. David Bergeron
Mumbai

FINANCIAL SERVICES

MARSH & McLENNAN COMPANIES

CONFIDENTIALITY

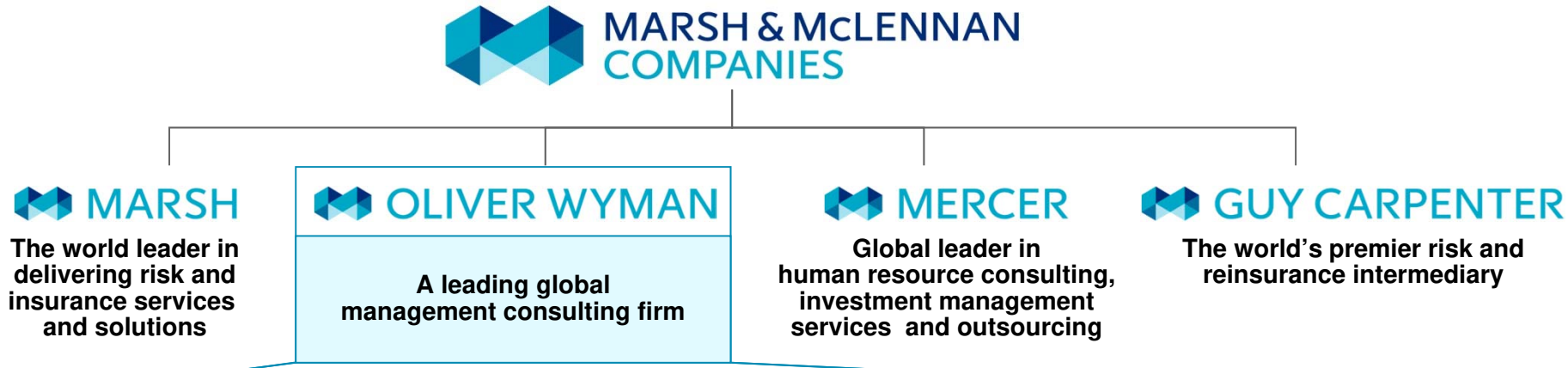
Our clients' industries are extremely competitive. The confidentiality of companies' plans and data is obviously critical. Oliver Wyman will protect the confidentiality of all such client information.

Similarly, management consulting is a competitive business. We view our approaches and insights as proprietary and therefore look to our clients to protect Oliver Wyman's interests in our proposals, presentations, methodologies and analytical techniques. Under no circumstances should this material be shared with any third party without the written consent of Oliver Wyman.

Contents

Section 1 | Introduction to Oliver Wyman

Oliver Wyman is a leading consulting firm in financial services and is the management consulting arm of Marsh & McLennan Companies

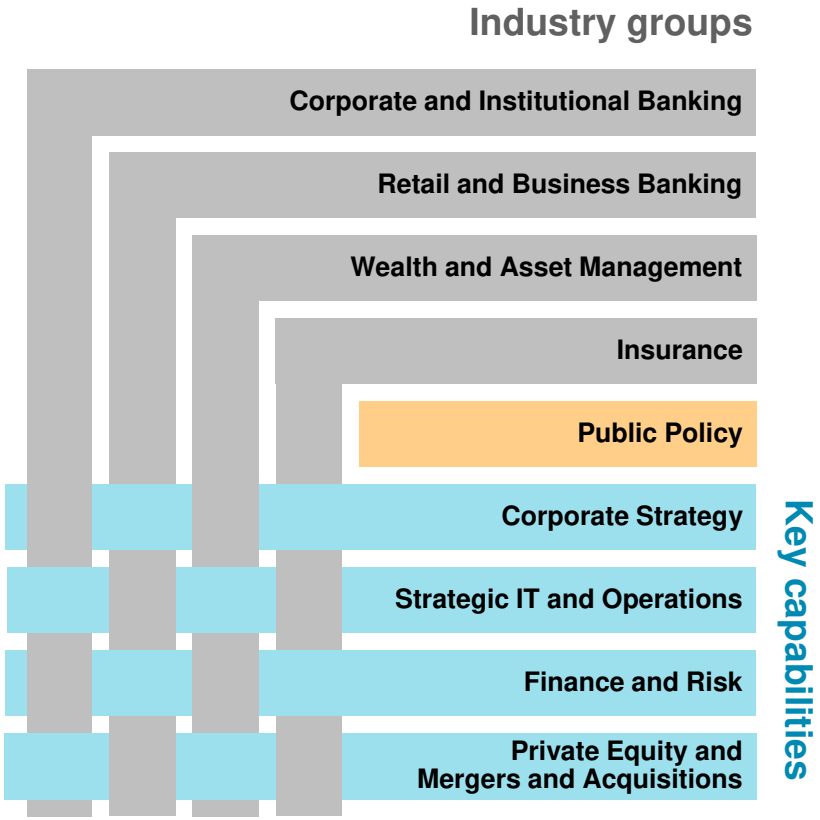


About Oliver Wyman

- Oliver Wyman group is a Top 3 global management consulting group with $1.5 BN in revenue and ~3,200 consultants working over 80 countries
- Number 1 consulting firm in quality (source: Corporate Executive Board Survey 2011)
- Number 3 in size and fastest growing among top-five global consulting firms (source: HBS 2009)
- Three key differentiators
  - Sector specialisation
  - Combine strategy and execution
  - Deep analytical and technical expertise

Oliver Wyman Financial Services brings penetrating industry expertise and broad functional knowledge to financial services clients

Oliver Wyman Financial Services key practices



Leading strategy consulting firm dedicated to financial services strategy and risk

- Dedicated and specialised practices within financial services
- Work with global leaders, including the majority of top 150 financial services firms as well as public bodies
- More than 1,200 staff in North and South America, Europe, the Middle East and Asia Pacific – 34 offices in 14 countries

Our approach is content-led, based on technical expertise and industry knowledge

- Deep analytical and technical expertise – heritage of the firm to produce new insights
- Industry knowledge – reinforced by financial services focus and global operating model, including financial services arms of industrial and automotive firms
- Impact – experience and processes to get things done in large and complex organisations

Our specialist practices give us a deep understanding of industry and supervisory perspectives

Oliver Wyman's Public Policy practice

Advisor of choice for global supervisors

- Organisation and governance
- Strategic planning and resourcing
- Risk governance and management
- Financial stability frameworks/processes
- Regulatory policy and supervisory practices
- Crisis management
- Reserve management

Oliver Wyman's Finance and Risk Practice

Leading global thinking in risk management

- Risk quantification, policies and processes
- Capital, funding and balance sheet strategy
- Accounting analytics, policy and implementation
- Regulatory compliance
- Organization design and governance

We have done > 140 dedicated operational risk projects for > 65 clients since 2003, including > 15 AMA banks and > 20 banks working towards AMA

Type	Approx. number of clients
Framework foundation setting	> 15
Full end-to-end framework build	> 10
Operational risk review/validation	> 40 (incl. validation of > 10 AMA models)
Management reporting	> 20
Integrated OR control framework build (ORM and other 2nd line functions)	~10
Key risk/scenario identification and analysis	> 20
RCSA builds	> 10
Loss data collection tools and processes	> 10
KRIs and KCIs	> 20
Operational risk capital calculation and allocation	> 20 (including 7 AMA model builds, 2 Solvency II model builds for major European insurers and several AMA-style model builds for banks not seeking AMA accreditation)

Section 2

Foundation setting

Overview of Operational Risk Management

What is Operational Risk?

Definition of key terms

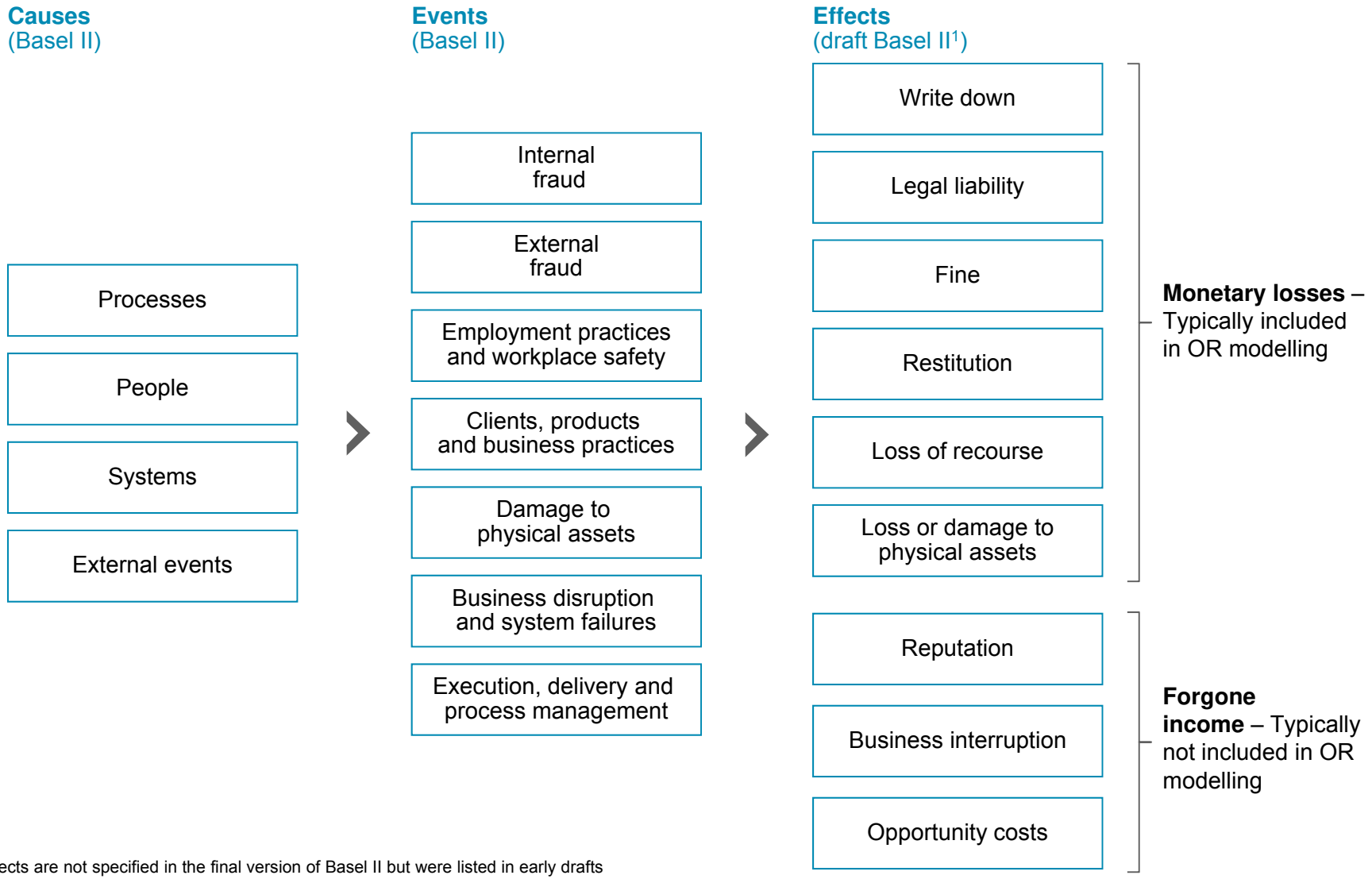
- **Operational risk (OR)** is "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events" including legal and HR risks (excluding strategic risk)
- In this sense, **OR events** are a subset of all risk events of the bank which have or likely have a negative financial or reputational impact
- The **cause of an OR event** is the factor responsible for the OR event to arise – for example, these factors can be categorised into processes, people, systems and external events
- The OR events themselves can be categorised into **event types** such as external fraud or business disruption and system failures
- The **impact of an OR event** is a specific outcome of the event – there can be financial consequences (loss or gain) as well as non-financial consequences (reputation loss or impact on staff morale)

Example high-level hierarchy of risk types

Basel L1 ▸ Basel L2 ▸ L3

- Internal fraud
- External fraud
- Employment practices and workplace safety
- Clients, products and business practices
  - Suitability, disclosure and fiduciary
  - Improper business or market practices
  - Product flaws
  - Selection, sponsorship and exposure
  - Advisory activities
    - Performance dispute
    - Mis-selling
- Damage to physical assets
- Business disruption and system failures
- Execution, delivery and process management

The universe of operational risks spans causes, events and effects
Basel II categories



1. Effects are not specified in the final version of Basel II but were listed in early drafts

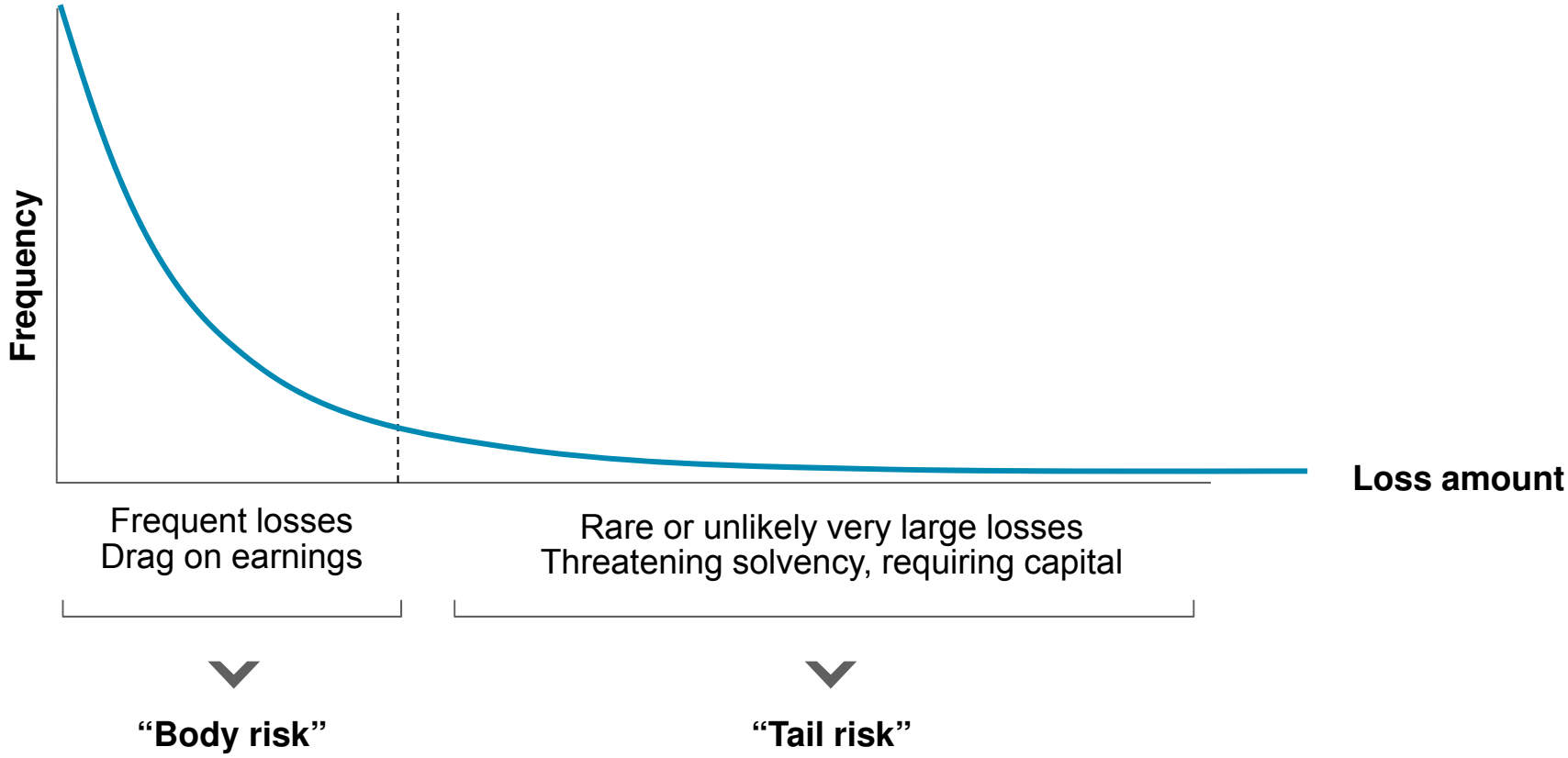
Operational risks are leading causes of bank failures

Examples of bank failures due to operational risk events

	Loss (US$BN)	Event type	Description
	~10	Loan fraud	Attempt to cover up loan loss during licensing process in UK, increasing exposure to both credit and market risks massively in the process. Bank collapsed following the incident. Settlements ongoing for ~12 years including law suits against other involved parties including the regulator
BARINGS	1.3	Rogue trader	Derivatives trading on Nikkei index, star trader in breach of limits in environment of poor controls. Bank collapsed following the incident. Event in Asia, though affecting Barings group wide
ธนาคารกรุงเทพ-พาณิชย์การ BANGKOK BANK OF COMMERCE	2	Internal fraud	Senior executives and advisers accused of fraudulent transactions and misappropriation of funds; some policymakers allege that BBC collapse triggered Baht collapse and subsequent Asian Financial Crisis

In most banks the leading operational risk types can lead to frequent losses as a drag on earnings, can present a rare but real threaten solvency, or a combination of both

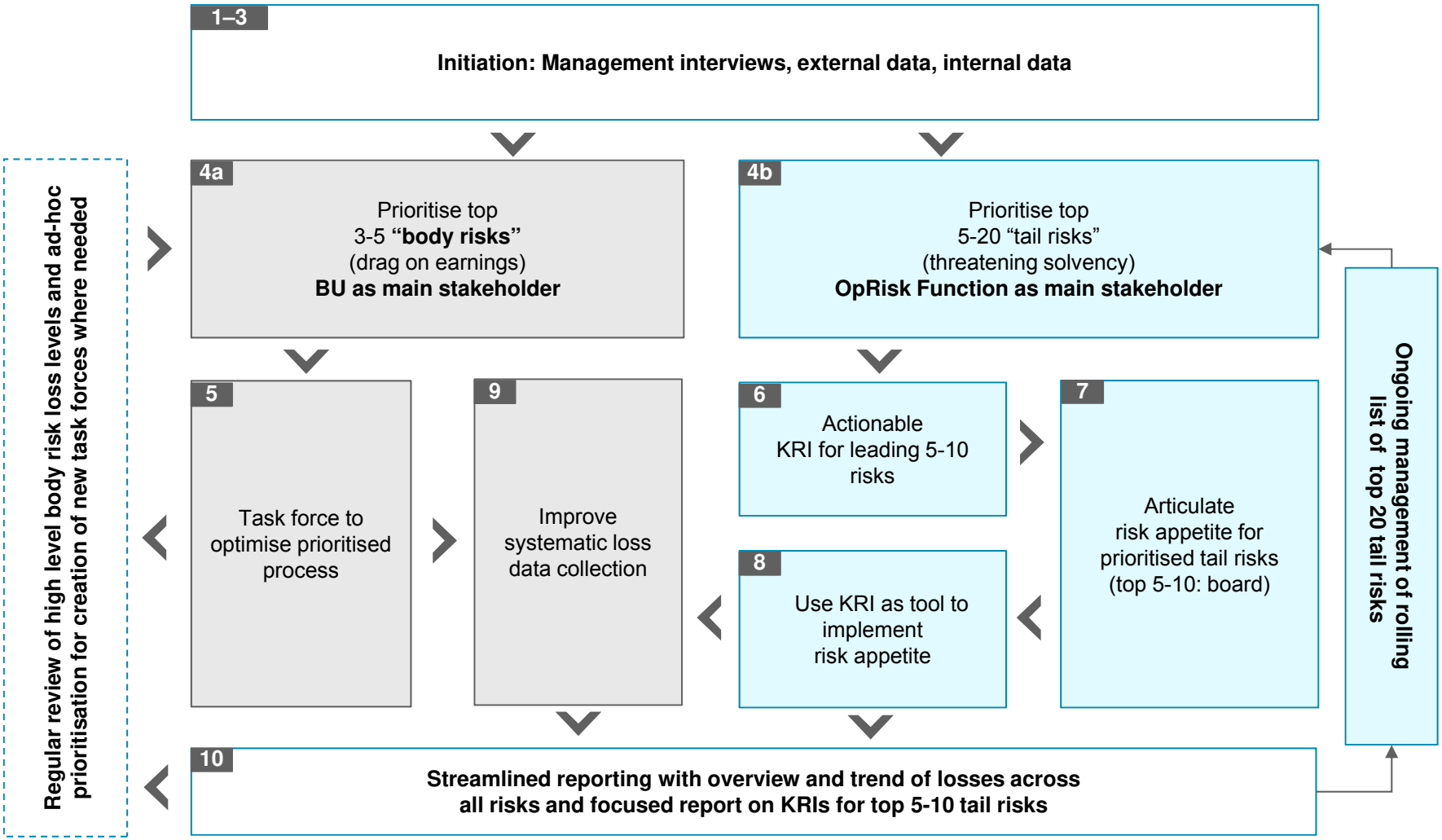
Illustration – Two components of the loss distribution



Body risks and tail risks need be managed differently

	Body risk	Tail risk
Examples	• Failure to enforce credit risk controls • Typical fraud losses	• Large scale sophisticated and rare fraud (~1-2 US$ BN) • Large scale client litigation (e.g. prompted by precedent law suit after exiting communicated credit lines) • Rogue trader
Management stakeholders	• Business units have key stake in reducing losses, as losses are a visible cost component • Risk as supporting function	• Operational risk management function responsible to articulate risk appetite trade off, monitor evolution of risk levels and implement controls in line with risk appetite • Board involvement in setting risk appetite for key tail risks

“Body risk” and “tail risk” management processes differ, as stakeholders are different – the operational risk function’s long run focus should be tail risks



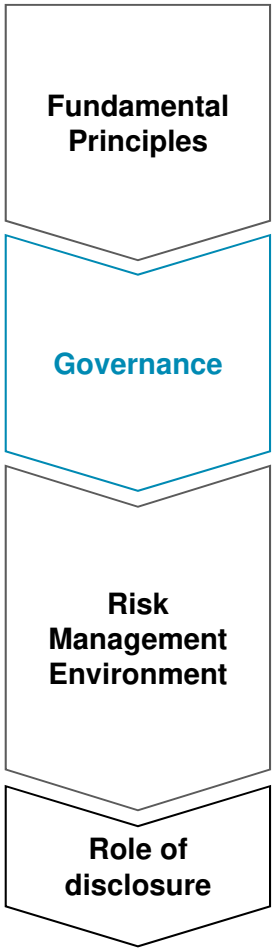
Section 5

Tools of the trade

Governance

BCBS lays out 11 principles for Operational Risk Management

Bank practices



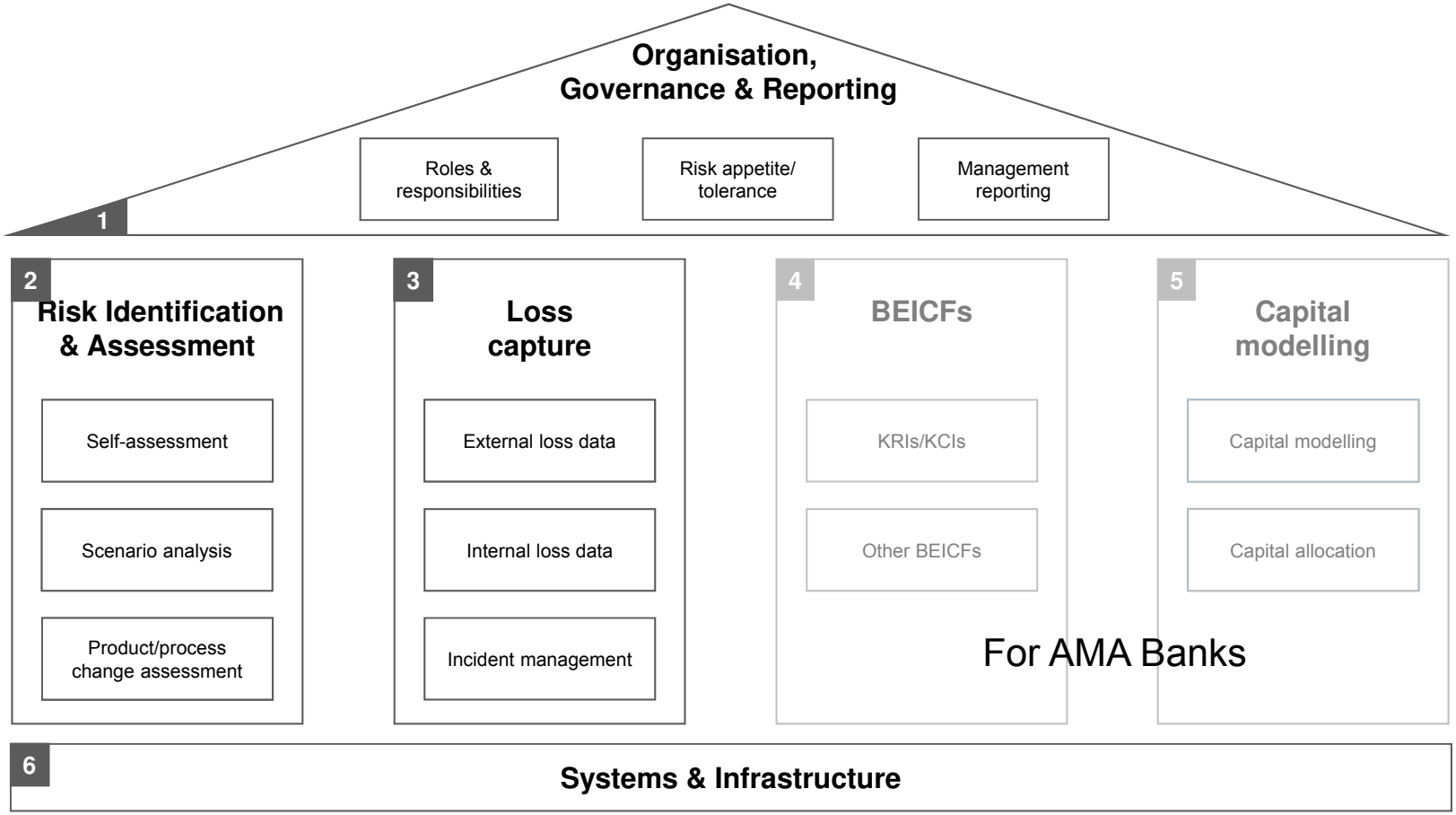
Principle 1	Board responsible for risk culture
Principle 2	Framework integrated in risk management processes
Principle 3	Board oversight
Principle 4	Board Risk Appetite
Principle 5	Senior management responsibility
Principle 6	Risk identification and assessment
Principle 7	Approval processes
Principle 8	Monitoring and reporting
Principle 9	Control and mitigation
Principle 10	Business resilience and continuity
Principle 11	Role of disclosure

Supervisory practices

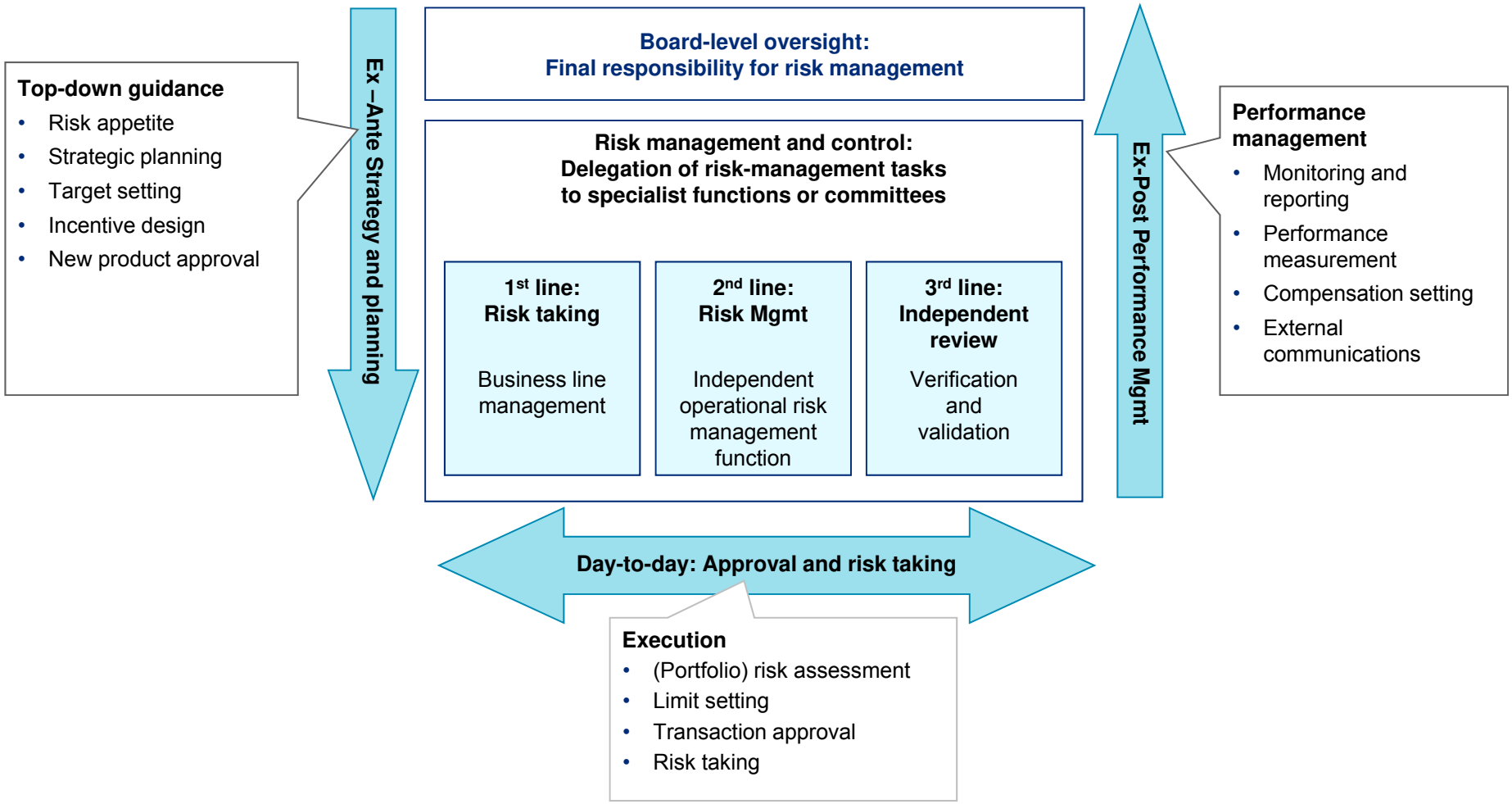
"Principle 25 – Operational risk: The supervisor determines that banks have an adequate operational risk management framework that takes into account their **risk appetite, risk profile** and **market and macroeconomic conditions.** This includes prudent policies and processes to **identify, assess, evaluate, monitor, report** and **control** or **mitigate** operational risk on a timely basis." 2

Sources: BCBS: Principles for the Sound Management of Operational Risk , June 2011, Core Principles for Effective Banking Supervision, Sept 2012

Components of operational risk management



Risk governance should follow a “three lines of defence” model, with the board exercising strong oversight over risk taking



The bank's articulation of its Risk Appetite should be the starting point for any risk management framework

Risk appetite
Tolerance for risk

How much risk can I afford to take without excessively exposing the business to potential financial distress?

Risk appetite defines the absolute downside risk beyond which I have no appetite for risk

Risk/control trade-off

How much will it cost to control the risk; is this more than the cost of accepting the risk?

Risk appetite considers the costs and benefits of controlling risks to maximise efficiency of risk taking

Articulation of trade-off

How can I articulate the acceptable level of risk to hold the business accountable?

Where risk reduction is desired clearly articulate performance indicators (KRI) and targets

Risk management options

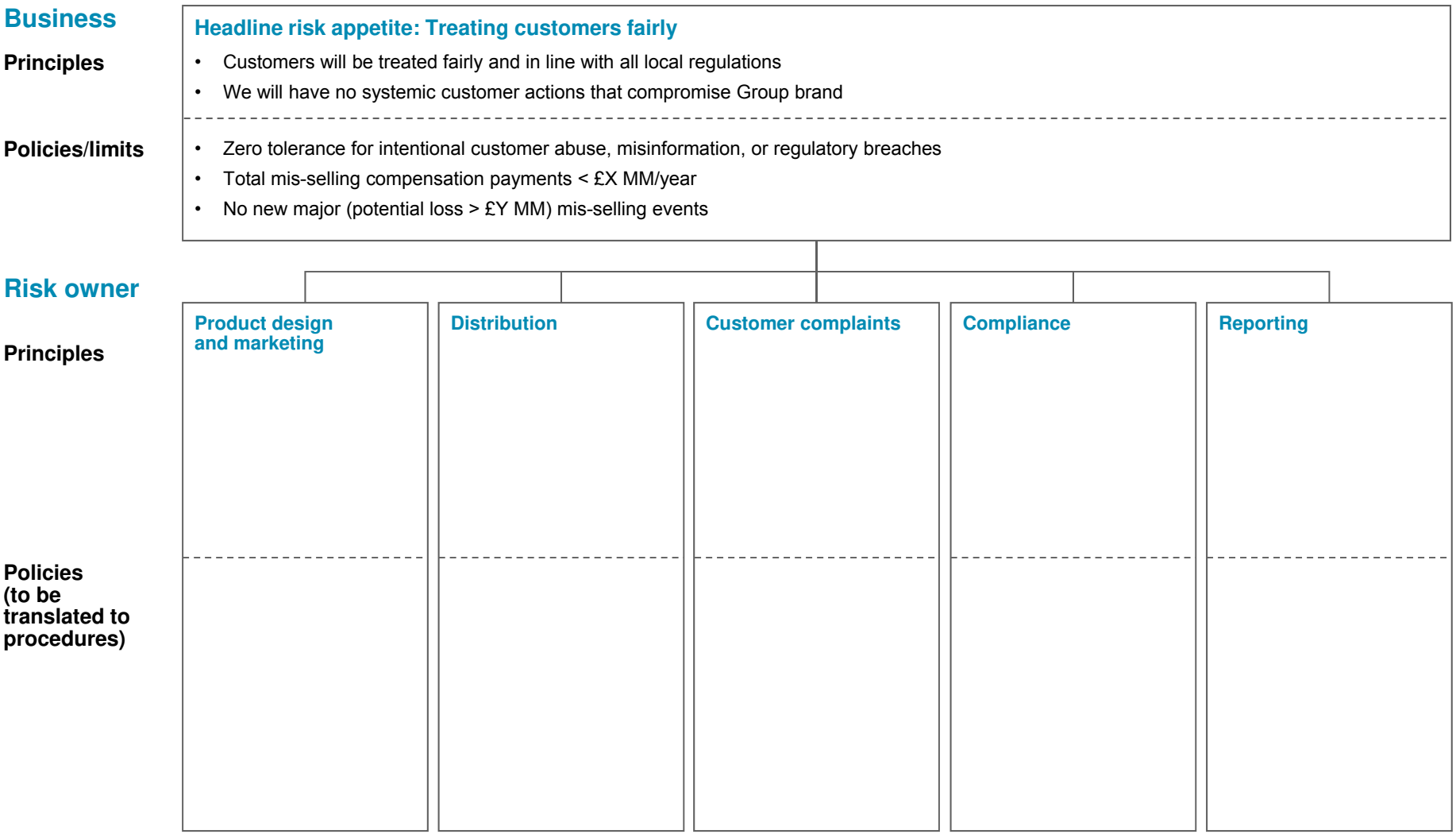
- **Reduce** the risk, through improving controls
  - Reduce the likelihood of the risk occurring and/or
  - Reduce the impact on the business should it happen
- **Accept** the risk, where the potential impact is less than the cost of control required to reduce it
- **Transfer** or **avoid** the risk
  - Transfer: contractually moving the responsibility or consequence of the risk outside the organisation (e.g. insurance, outsourcing)
  - Avoid: choosing not to operate in certain markets/products etc.

Banks would typically pick from the following six dimensions when formulating their operational risk appetite statements

1. Not exhaustive

Client example

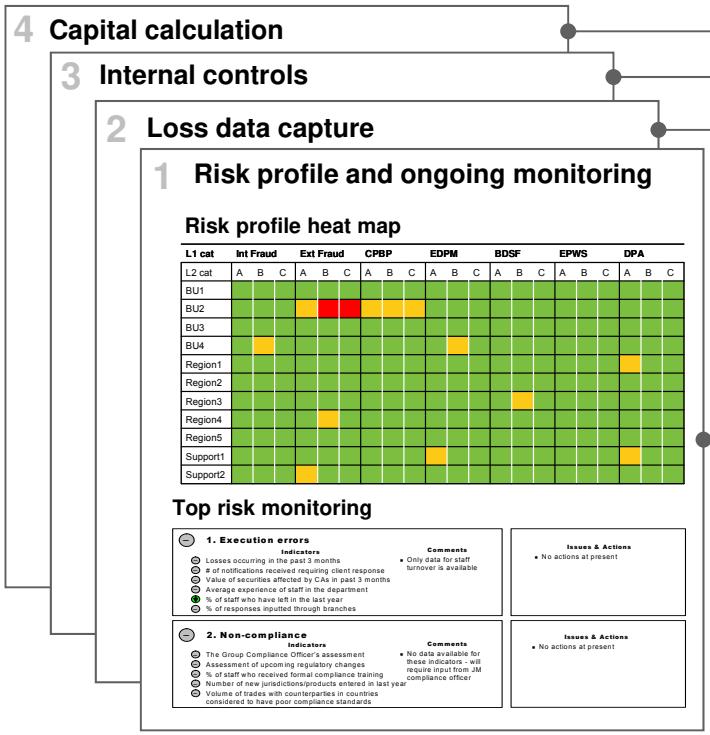
Risk appetite/tolerance statements for top risks can be translated into principles and policies to ensure that risks are managed within tolerance



Client example

Management reporting should be succinct, targeted, decision-oriented and clearly linked to risk appetite/tolerance

Example reporting components



Main contents

4
- Reporting on operational risk capital for group and per business unit and region
- Report on main underlying drivers

3
- Control reports
- Action plans

2
- Internal loss data reports
- Briefing memos on external "case study" incidents

1
- Heatmap
- Top risk summaries
- Regular risk MI reports, e.g. KRIs

For prudential supervisors, reports can be essential source of insight into the quality of information and degree of management response

Capital has generally not been a successful incentive mechanism for operational risk, and can usefully be to be complemented by more “hands-on” approaches

- Balanced scorecards
  - KRIs for large operational risks and
  - Typical operations KPIs
  - Actual losses incurred
  - Audit and Compliance input (if possible to do with existing systems)
- Put scorecards or equivalent in objectives for BU managers and link to remuneration
- Broader awareness raising initiatives. Examples used include
  - Group-wide project on clarifying risk drivers for a class of risks which sits in many BUs, and set new minimum standards
  - Emails or newsletter communication alerting employees to dangers triggered by specific external losses or general trends (rises in for instance external fraud levels etc.)
- League tables
  - Based on internal loss data and/or KRI performance with senior management praise for the “top performers” (and possibly publication of overall league table)

These mechanisms have the additional benefit that they can be targeted at both risk and loss reduction at the process level

‘Specialised’ risks represent potentially catastrophic impacts which far outweigh their direct financial impact

1 **Reputational risk**

2 **Business disruption risk**

3 **Information security**

3 **Compliance risk**

- Many institutions deploy separate frameworks for these risks given their importance and specialised mitigation actions
- Leading firms recognise the synergies / linkages between risks and hence coordinate ORM practices such as scenario analysis
- Some firms employ a unified framework where ‘impact’ assessment captures impact across reputational, business continuity etc.

Section 4

Tools of the trade
Risk Management environment

Banks employ structured frameworks for management of operational risks which employ similar key elements

- Identify key risks by operational area for each business unit using multiple data inputs
- Prioritisation of the risks to identify key risks

- Explore causes of vulnerabilities and identify root cause(s)
- Assess controls against what could go wrong (use frequency, severity, control effectiveness ratings)

- Brainstorm long-list of possible approaches to address causes; consider accepting risk, controlling risk, mitigating risk
- Prepare short-list of control options and develop business case for controls/mitigation improvements
- Develop Key control indicators (KCIs)
- Develop the reporting and MIS including KRIs for each risk

- Action Plan presents detailed implementation plan for recommended mitigation
  - Required resources and costs
  - Proposed work plan
- Risk parameterisation and op. risk capital modeling

- Project sponsor signs off on action plan
- Each plan is allocated an owner, project team and supporting resources
- The roles and required commitments of all supporting resources are clearly specified
- Implementation progress should be monitored against the action plan through an overall status indicator

Several standard frameworks are used to provide structure to ORM frameworks – regardless of framework, effectiveness depends on implementation

Overall frameworks and certifications

- "Enterprise Risk Management"
  - COSO
  - ISO 31000
  - Proprietary vended or internal ERM frameworks
- RCSA processes
- Business Continuity
- Information security
  - CoBIT

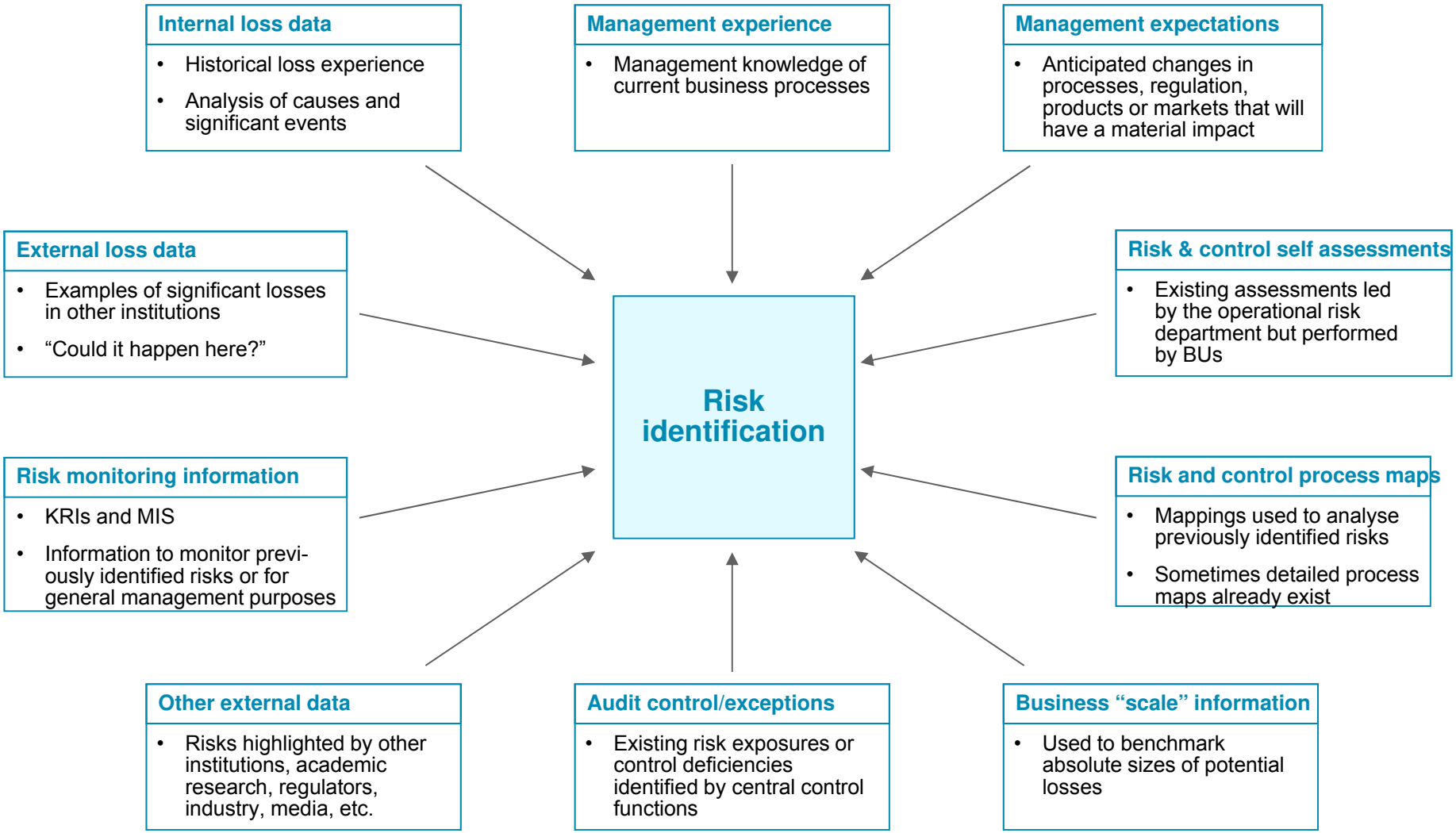
Implementation questions

- Is the framework well suited to the nature of risks faced by the bank?
- Is the framework effectively linked to the Risk Appetite of the board?
- Is ownership sufficiently devolved to the functional areas to enable effective identification and control?
- Does the implementation adequately address existential threats presented by tail risk, and not just everyday leakage containment of body risk?
- Does the prioritisation framework elevate the 'right' risks to management attention? (ie: from supervisory perspective, the salient existential risks)
- Is there sufficient oversight of framework implementation constituent models?

Success is less dependent on framework used than its implementation

Accountability and responsibility • People **must** take ownership of the risks in their area	›	• The central operational risk function cannot "own" or manage all the risks in the bank • Operational risk impacts the bottom-line of all business units and should therefore be a priority
Acknowledgement of risk • Operational risk is generated by all people and all processes, it can **never** be eliminated	›	• Exposure to operational risk is not something to be avoided at all costs, it is a by-product of running the business
Pragmatic risk/control trade-off • Banks **must** understand their appetite for each type of operational risk event	›	• If risk appetite is set at zero then the business will cease to operate • If the cost of control is greater than the cost of accepting the risk, why is the control in place?
Open risk-taking culture • People **must** be encouraged to report errors and weaknesses, to enable preventative measures to be taken	›	• Losses **will** occur; there may not be someone at fault • If people are punished for being open with their risks and losses then this negates the entire purpose of the operational risk framework
Risk empowerment • People **must** be given the ability and the mandate to manage their risks	›	• People will not feel that they own their risks unless the authority to manage their risks and controls has been delegated

For rigorous top-down risk identification and assessment all available data sources are taken into account



RCSAs are long-established and a cornerstone of OR identification, assessment and management, but there is often scope for improvement

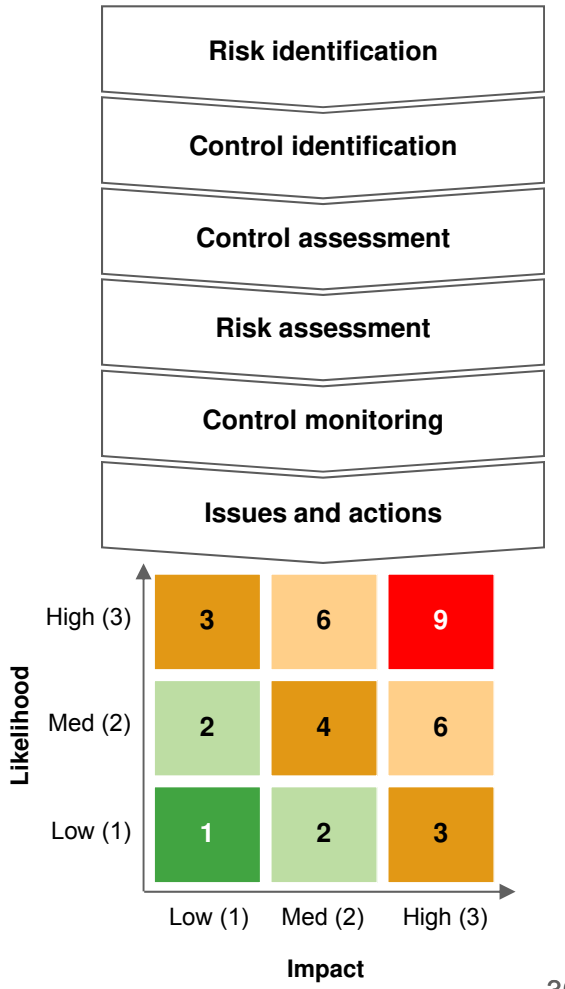
Role of RCSAs (Risk and Control Self Assessments)

- RCSAs are the premier tool for identifying and assessing operational risks, not only across the ORM community but also across the business and specialist functions such as Compliance, BCM, IT, HR etc.

Present challenges

- Ensuring consistency of outputs and the appropriate focus across risk types, while catering for BU and Group-function specific needs
- Finding an appropriate level of granularity
- Maintaining quality of inputs, process and outputs, over time
- While a degree of variability in the quality of RCSAs is inevitable, banks have spent significant effort recently to improve this, and tried different approaches to ensure high quality and consistency across their RCSAs
- How to aggregate RCSA results and report them
- Whether to take a process or risk-based approach

Example RCSA process



Banks seek to overcome these challenges by soliciting right inputs, in a structured approach underpinned by a robust governance framework

Right inputs

- Comprehensive involvement and cooperation across all relevant BUs and functions
- Accurate capture of full breadth of perspectives

Structured approach

- Structured approach for
  - identifying potential KRI/KCIs for monitoring
  - capturing the full range of risk drivers, impact and controls
- BU ownership of mitigating actions

Robust governance

- Robust challenge/verification process
- Robust monitoring, approval and escalation processes to ensure actionable outputs

Key controls are also identified through workshops and KCIs put in place
Key controls example for the risk “execution errors”

		Effectiveness	
Data field	**Controls**	**Potential**	**Actual**
Preventative controls Description	• Staff training/awareness	L	2
	• Emphasise to staff the importance of avoiding errors	L	2
	• Process automation and checks	H	1
	• Staff incentivisation	L	4
	• Staff supervision	L	2
Detective controls Description	• Random checks	L	4
	• Risk monitoring information which provide early warnings of a risk materialising so that prompt action can be taken	H	2
	• Senior staff should examine high impact operations	M	2
	• Staff must check reports that show execution errors and impacts	L	1
Mitigatory controls Description	• Spare resource allocated to fix errors	M	4
	• Reconciliation process at half- and end-day and before key systems closure (e.g. international payments)	M	2
Potential control improvements (vs. current situation)	• Increase intermediate checks for more critical operations	H	3
	• Operations reviewed by a second “eye”	L	0
	• Develop automated system that will reduce the options of clerical mistakes	M/H	2
	• Increase training for staff and explain impact of errors	L	2

Effectiveness scales

- **Potential:** This is a measure of how much this type of control could reduce the risk (i.e. the effectiveness of the control if it is working to its maximum potential)

	Potential impact
High Medium Low	Qualitative assessment of the effectiveness of the control

- **Actual:** This is a measure of the how much the current control is reducing the risk (i.e. how effective is the control currently)

		Actual impact
4	Very deficient	No control mechanism or with zero efficiency
3	Deficient	Control mechanism with limited efficiency in risk mitigation
2	Normal	Control mechanism with sufficient efficacy in some cases
1	Adequate	Efficient control mechanism in majority of cases where the risk could have materialised
0	More than adequate	Efficient control mechanism in all the cases where the risk could have materialised

- Control data has not been available, so the controls shown in this table are for illustration purpose only

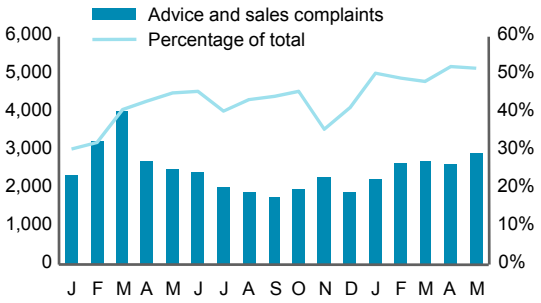
1. High level impacts that apply to all the process

The industry still struggles with KRI/KCIs – in our experience they are best defined sparingly and tied to top risks

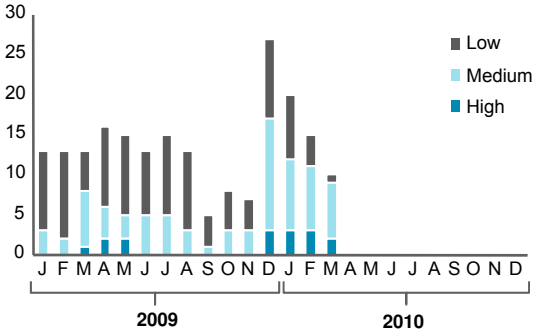
- KRI/KCIs
  - Capture trends in operational risks – often measured as **red**, **amber** or **green**
  - Don't give the level of operational risk capital
- The industry still struggles with KRI/KCIs because they are
  - Costly to collect
  - Difficult to define (especially across BUs)
  - Difficult to back-test against "tail" events because of the scarcity of the latter and hence have to be chosen mostly on the basis of a belief that they are linked to the risk
- In our experience, KRI/KCIs are best chosen selectively to represent information you would bring to a Board/ExCo meeting if you had to comment on developments in a given risk
- Because they are recognised as being inherently useful, we see greater focus on KRI/KCIs now than ever
- Half of AMA banks use KRI/KCIs directly or indirectly in their models[1]
  - Audit scores are frequently used

Client examples of KRI/KCIs

↑ Complaints – advice and sales



↓ "Open" control issues from BCM assurance reports



1. BCBS, Observed range of practice in key elements of Advanced Measurement Approaches (AMA), July 2009

Section 3

Operational Risk Capital
Basel II approaches

The Basel II Basic Indicator and Standardised approaches are used by most banks in emerging markets for assessing operational risk capital…

Basic Indicator approach

$$K_{BIA} = \left[\sum GI_{1\ldots n} \times \alpha\right] / n$$

where:

K_{BIA} = The capital charge under the Basic Indicator Approach

GI = Annual gross income, where positive, over the previous three years

N = Number of the previous three years for which gross income is positive

α = 15%, which is set by the Basel Committee, relating the industry-wide level of required capital to the industry-wide level of the indicator (12% of total capital)

Standardised approach

$$K_{TSA} = \left\{\sum_{\text{years } 1-3} \max\left[\sum \left(GI_{1-8} \times \beta_{1-8}\right), 0\right]\right\} / 3$$

where:

K_{TSA} = The capital charge under the Standardised Approach

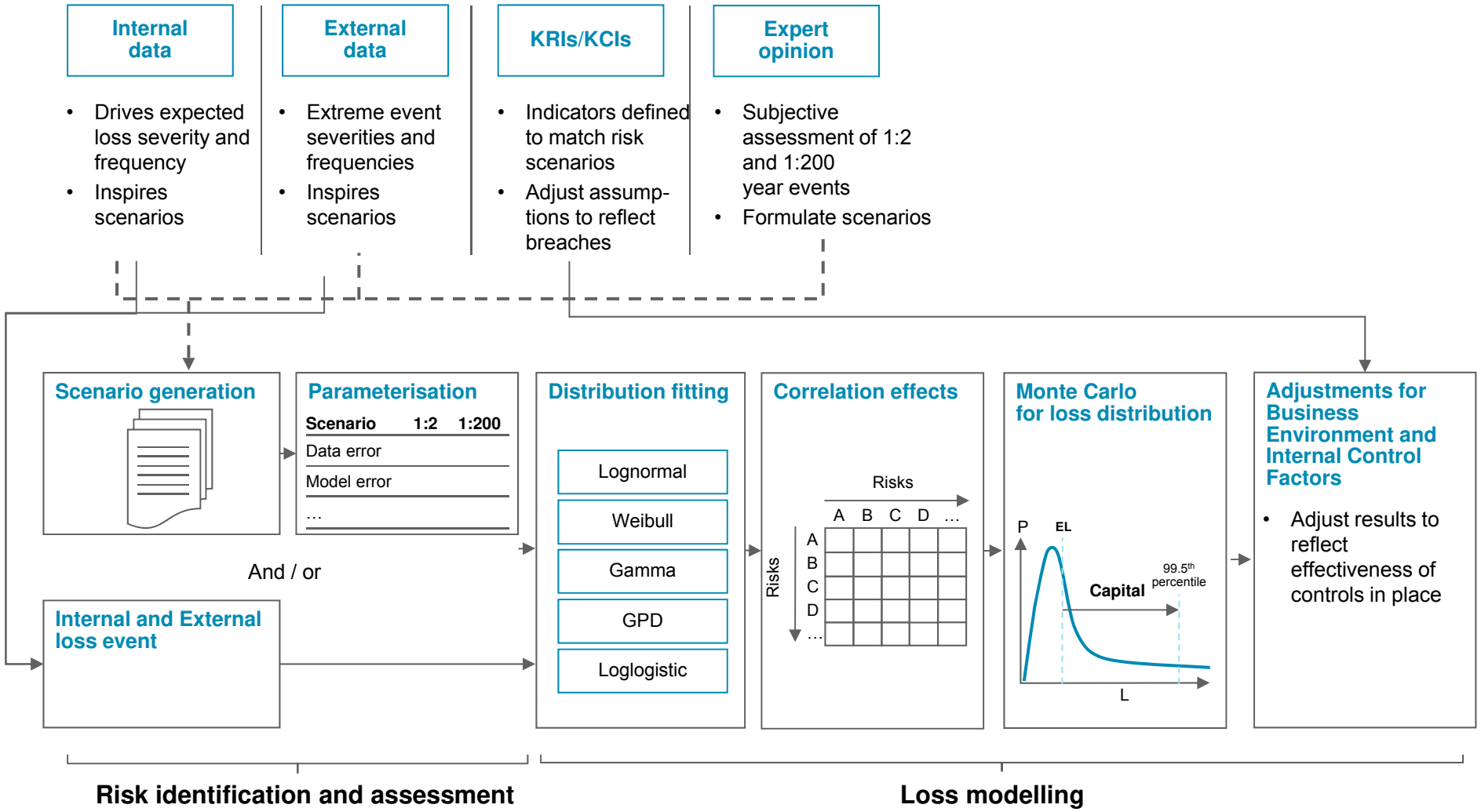
$GI_{1\text{-}8}$ = Annual gross income in a given year, as defined in the Basic Indicator Approach, for each of the eight business lines

$\beta_{1\text{-}8}$ = A fixed percentage, set by the Basel Committee, relating the level of required capital to the level of the gross income for each of the eight business lines

Business line	Beta	Business line	Beta
Corporate finance	18%	Payment and settlement	18%
Trading and sales	18%	Agency services	15%
Retail banking	12%	Asset management	12%
Commercial banking	15%	Retail brokerage	12%

… although the number of AMA banks is steadily increasing

In the AMA modelling approach, key risks need to be quantified under various scenarios and adjusted for control factors to arrive at expected losses



Scenario analysis has become a bone of contention, especially in the US, but it **is** useful for both management and measurement

	Scepticism	Support
Key points/ concerns	• **Subjectivity** and **error margins** involved in estimation of LFHS events • Potential for **"gaming"**	• **Only forward-looking and institution-specific input** available to determine capital requirements • **Simplicity** and **transparency** of SBA modelling – direct linkage created between accepted risks and capital, thereby strengthening **incentives**
Geographical prevalence	• Prevalent in the **US** – Loss data is relatively abundant – Rare for US banks to give SA significant model-endogenous weight in determining the bank's overall capital number… – ….although SA is frequently used as a back-end check on the LDA numbers, with the potential to adjust LDA numbers upwards	• Although views outside the US are mixed, this view holds sway with many banks and regulators **outside the US** – Loss data is less abundant outside the US – Scenarios are more widely used as direct model inputs with significant impacts on final capital numbers outside the US

This dichotomy is troublesome (but not insurmountable) for large, internationally active banks subject to AMA requirements in the US and elsewhere as they face the prospect of building one model for the US and one for the rest of the world

There are several challenges in implementing and validation of AMA models which are particularly acute in emerging markets environment

- Scarcity of (relevant) **External Loss Data (ELD)**
- Relatively short history of **Internal Loss Data (ILD)** at many institutions
- Institution of robust **loss data capture** processes
- Design and incorporation of robust **Scenario Analysis** frameworks for comprehensive capture of risk exposures across event categories
- **Correlations**
- **Business Environment and Internal Control Factors (BEICFs)**
- Ensuring the model is **appropriately risk and control sensitive**

Business Environment and Internal Control Factors (BEICFs) become cornerstones of many banks' OR capital and OR management frameworks…

- Typically, banks take BEICFs to refer to one or more of the following
  - Risk and Control Self Assessments (**RCSAs**)
  - Key Risk Indicators (**KRIs**) and Key Control Indicators (**KCIs**)
  - **Audit points**/scores

- These are often regarded as **cornerstones of the operational risk management framework**
  - Especially RCSAs, which are found in the vast majority of banks in some shape or form

…but the use of BEICFs in capital models tends to be crude

- Strictly speaking, many AMA banks **do not live up to the Basel II requirements for BEICFs** used in models to be
  - Meaningful drivers of risk
  - Capture both risks and controls
  - Validated through comparison to internal and external loss data
- …although this is **improving** over time
- However, the number of banks **incorporating BEICFs** as a separate class of elements in their models has been increasing over the last half decade
  - More than 2/3 of AMA banks use them as indirect inputs (i.e. to inform/validate other inputs such as scenario analysis)[1]
  - Only 1/7 AMA banks uses them as a direct input that affects the bank's overall AMA capital[1]…
    - 1/14 as a direct model input[1] (e.g. RCSAs as a kind of scenario analysis, scenario parameters based directly on KRIs)
    - 1/14 as an ex-post adjustment[1] (typically via scorecards)
  - …although 1/6 use them to adjust allocation to business level[1]

1. BCBS, Observed range of practice in key elements of Advanced Measurement Approaches (AMA), July 2009

For many AMA banks, extracting more value from ORM is a key concern – Example initiatives from our recent work (1/2)

- **Focusing on the top risks**
  - Clear identification, assessment and quantification of the top risks, ideally with transparent and material linkages to capital numbers
  - Clear business cases for controls improvement via cost/benefit analyses
  - Focus on following through on mitigation actions
- **Mining internal loss data** to determine root causes and drive down losses – examples from recent Oliver Wyman experience include
  - A global universal bank that reduced annual credit-related op risk losses by $100 MM (40%) in one of its regions through a handful of simple initiatives
  - A European universal bank that similarly reduced its annual op risk losses by >€100 MM (30%)
  - A Nordic bank that reduced deal capture errors in its relatively small Markets division by €1 MM per year through a narrow but targeted effort
- **Setting non-capital incentives** to supplement capital-based incentives, which are often weak
  - Balanced scorecards providing a link between ORM and remuneration
  - Targets based not only on capital but also KRI/KCI/KPIs and losses
- **Providing an operational risk voice in a number of key business decisions**
  - New product approval – pretty mainstream now
  - Outsourcing – less common
  - Strategic and business planning – rare

For many AMA banks, extracting more value from ORM is a key concern – Example initiatives from our recent work (2/2)

- **Taking the lead on wider risk management and control initiatives** (which can be very useful as long as it does not distract unduly from the core mission of ORM)
  - Risk-adjusted compensation (especially KRIs and "knocks-outs" due to breaches of risk and compliance requirements)
  - Reputation risk and business risk
  - Emerging risks and Enterprise Risk Management
  - Integrated controls management
- **Assuming responsibility for "adjacent" functions historically housed elsewhere** (which has a mixed record)
  - Insurance purchasing
  - BCP and other "specialist risk functions", including Compliance in some cases
  - Internal Control
- **Improving co-ordination and co-operation with "adjacent" functions** to achieve better risk management at lower cost and with less business disruption – typical areas for improvement include
  - Common risk taxonomy/language
  - Shared risk identification and assessment processes
  - Consolidated and streamlined reporting
  - Shared databases capturing risks, controls, issues and actions
  - Clear "risk owner"/"risk SME" model providing clarity about roles and responsibilities and providing an opportunity for systematic tapping of specialist knowledge

Section 6 | Recap and Questions

We can learn from the experience of leading banks in their early ORM implementations

Common pitfalls

- Excessive focus on granular data capture and modelling which does not inform better management
- Early focus on lengthy “tool” development e.g. KRIs, RCSAs, process mapping, without it being properly integrated
- One-off project of 1-2 years driven by Group; not embedded in business-as-usual nor adding benefit to front-line
- Requesting information from businesses which is already collected by other control functions (compliance, audit, etc.)
- Belief that if you have an OR manager in place, you have “solved the problem”
- Aiming for theoretical perfection rather than operational effectiveness

Keys to success

- Take a pragmatic approach to measurement; build from drivers rather than (only) losses
- Get a framework in place that shows early tangible risk and cost reduction
- Design business implementation plans with understanding of existing structures and project ongoing in the BUs
- Work top-down, identifying key risks and focusing further investment on these
- Make sure you have a clear delineation between the responsibilities between OpRisk, Compliance, Audit, Legal, IT, Security, etc. for each major risk type

1. Sources: Oliver Wyman project work and surveys of leading banks in 2005, 2006, 2007 and 2012

Key takeaways

Operational risk is:

- Important
- Multi-faceted
- A young and developing discipline
- Often not given enough management attention
- Complex to assess
- Complex to manage

All institutions should have key basic tools in place

- Risk appetite/tolerance
- Risk identification and assessment processes (RCSAs, scenario analysis)
- Metrics (KRIs and KCIs)
- Management reporting
- Loss data collection and incident management procedures
- Operational risk input into key business processes, e.g. insurance purchasing, NPA, major business decisions etc.

Supervisors should look particularly at risk reporting to ensure that:
1) There is sufficient awareness of the top risks faced by the institution
2) Assessment of risk is followed up by concrete action

Any questions