



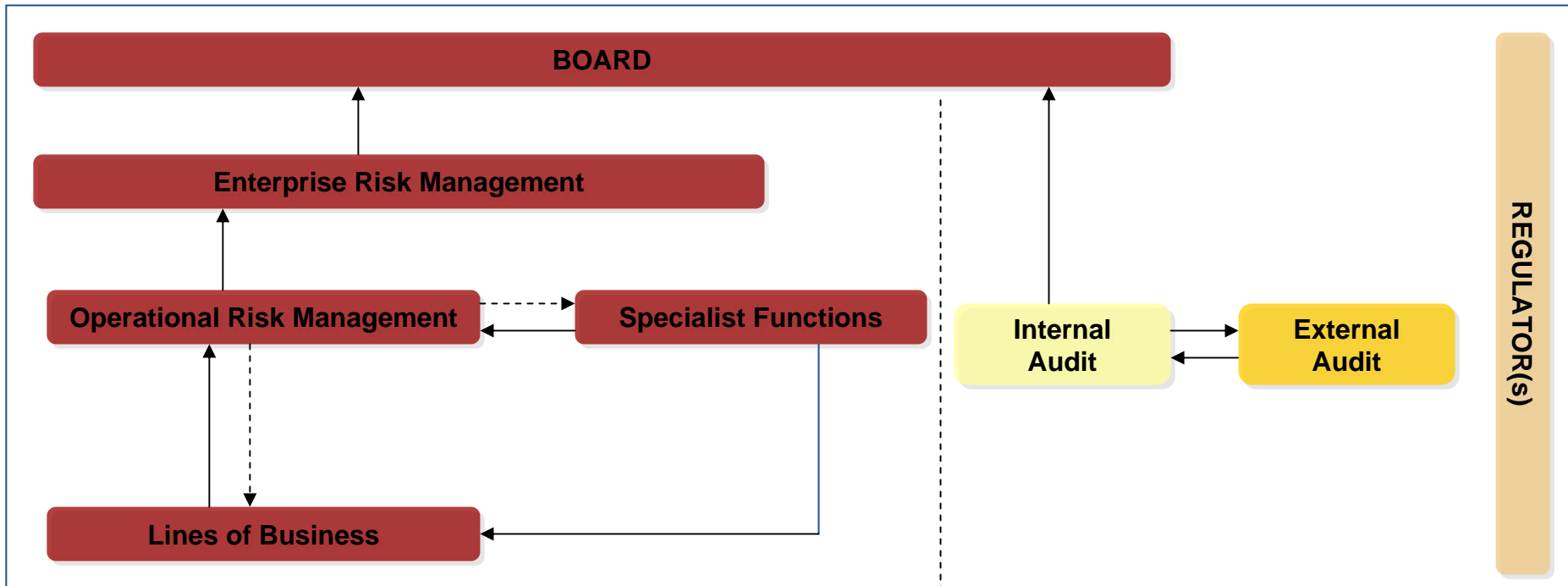
**Operational Risk
Management
Key Learnings over the
past decade**

**Malaysia
Tue, Jul 15, 2008**

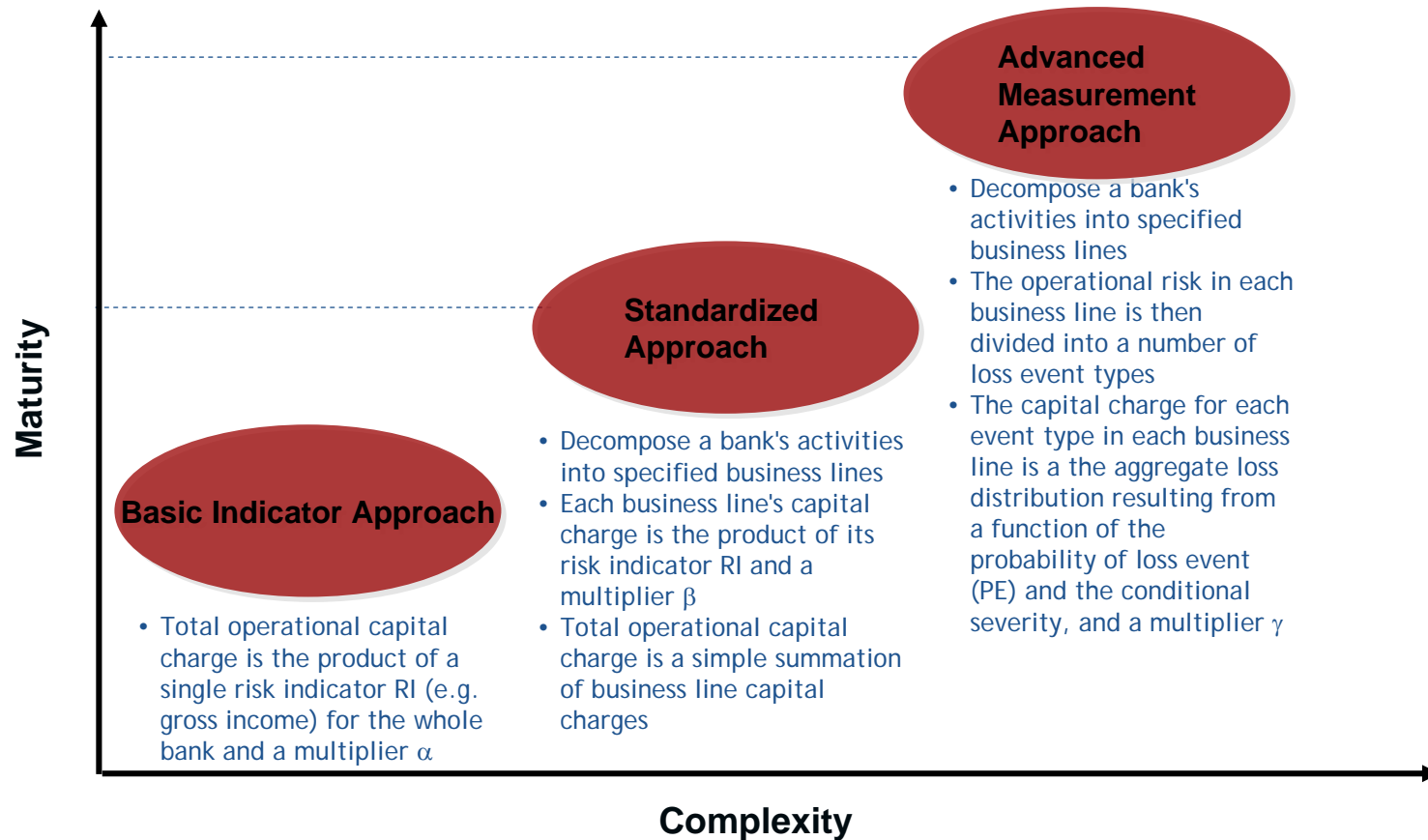
1. Overview
2. Operational Risk Management (ORM) Process and Method
3. ORM Building Blocks
4. ORM Data Analysis – a first level example
5. Determining Risk Appetite for an Entity

1. Overview

- **Firm specific**
- **Scope**
 - **Enterprise wide vs. centralized**
 - **Involved User Base**
 - **A risk manager: “We have 10 people in market risk, 100 in credit risk and 1000 in operational risk”**
- **Subjectivity involved**
 - **Data Capture**
 - **Capital estimation**



- ORM evolves from a traditionally siloed and fragmented approach to a defined governance model
- Decentralized identification, assessment, monitoring and reporting
 - Lob's, Specialist functions (incl ORM)
- Centralized oversight and support
 - ORM supports and facilitates, plus validates Lob information with specialist functions
- Independent Assurance by Internal Audit



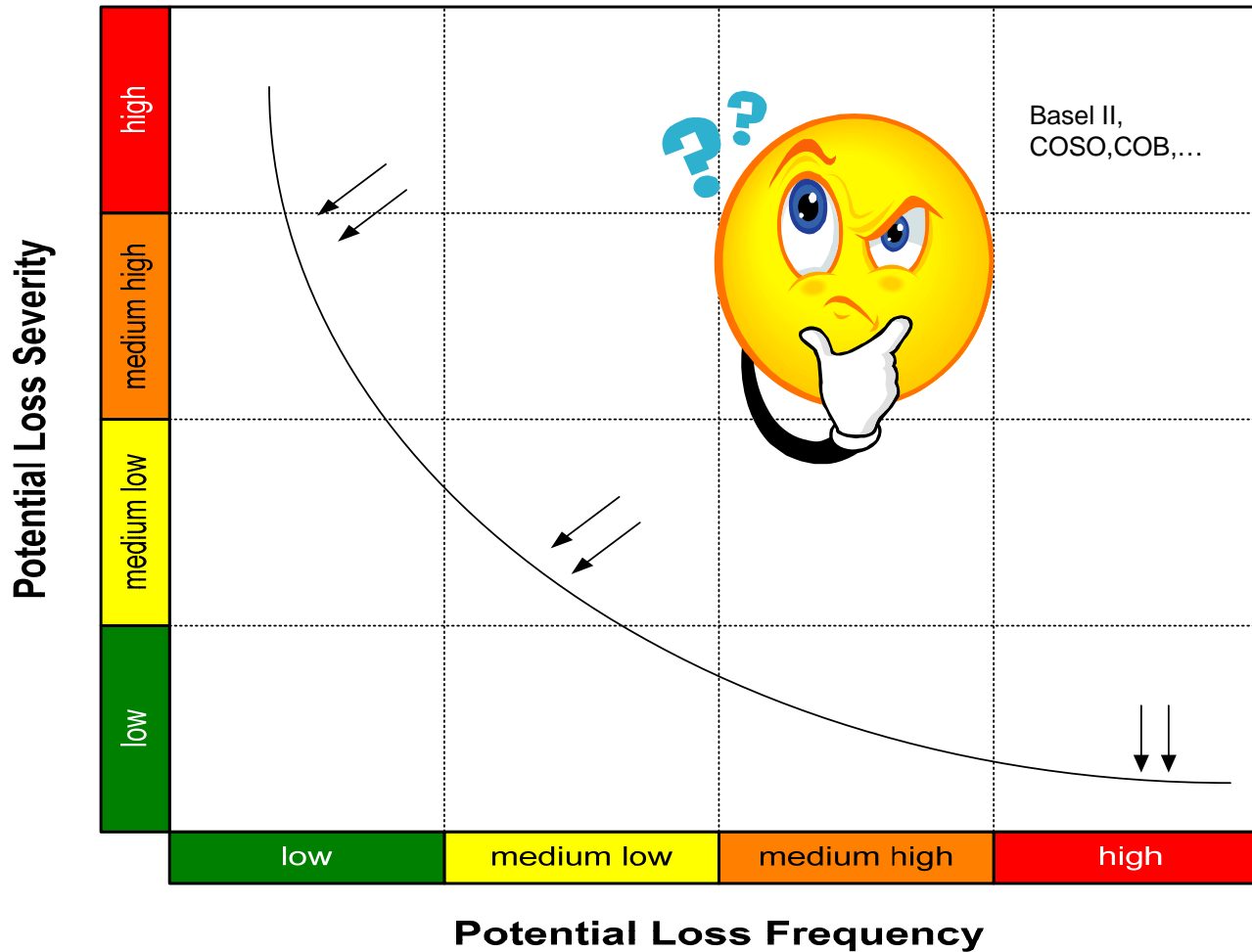
An organization needs to comply with progressively more rigorous criteria in order to progress from the basic indicator to an advanced measurement approach

It is vital that the dataset is complete, accurate and consistent, especially more so as the organization moves down the continuum of approaches

Approach	Gross Income	Risk Weighted Assets	Loss Data	Scenarios / External Loss Data	RCSA	KRI
Basic Indicator	Bank level					
Standardized	Per std Bus line		X		X	X
Alternate Standardized	Per std Bus line	For RB and CB	X		X	X
Advanced Measurement	Per std Bus line*		X	X	X	X

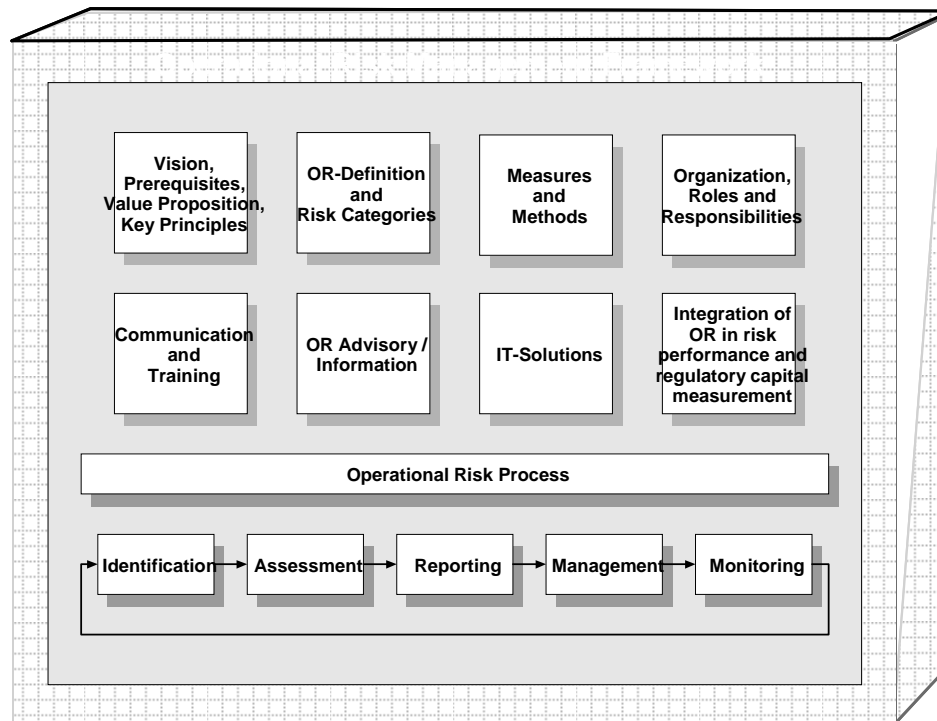
* Gross income is still required for AMA as a reference

- **What is the mandate?**
- **What is the approach? And realization?**
- **What is the budget and timeline to implement?**
- **What additional functional resource or data capability required?**
- **What are the infrastructure and technology requirements?**
- **Is any external consulting / training required?**
- **What will the delta in management structure and processes be over time, how will the change be managed?**



The need to prioritize mitigation efforts to optimize value add to Business while complying with the guidelines of multiple generally accepted frameworks that address multiple regulatory requirements

- **Governance model**
- **Policies and guidelines**
 - Policies include mandate, definitions, scope, roles and responsibilities, processes, reports, reporting lines and frequencies, information workflows, escalation triggers
 - Guidelines include decision trees, exception management, process mapping
- **Framework**



- **Confusion around mandate and objectives**
- **Inconsistent methodology and approach**
- **Inconsistent processes**
- **Inaccurate data and suspect analysis**
- **Challenging technology solution implementation**
- **Decrease in credibility and reduction in ORM potential to benefit the organization**
 - **Optimizing controls**
 - **RAPM**
 - **Market perception**
 - **...**

2. ORM Process and Method



Key stake-holders of an operational risk management process include

- Business
- General management (GM)
- Operational Risk Committee (ORC)
- Operational Risk sub-committee (Sub ORC)
- Global Risk Management (GRM)
- Local Risk Management (LORM)
- Centers of competence (e.g. Information security, disaster recovery team) (CoC)
- Audit
- Compliance
- Legal

For each step in the risk management process, individual stakeholder's activities are represented



Stakeholder	Business	GM	ORC	Sub-ORC	Global WRB	Local WRB	CoC	LORM	Audit	Compliance
Process / Activity										
Risk identification										
Provide framework to identify operational risks					Execute					
Approve framework			Approve							
Define RSA scenarios					Execute					
Approve scenarios			Approve							
Perform risk identification							Execute			
Assist in performing risk identification	Assist				Assist					
Review risk identification					Review				Review	
Approve risk identification		Approve								
Co-ordinate and plan risk identification							Execute			
Approve planning				Approve						
Report on status of risk diagnostic					Report			Report		

Key: ■ Execute ■ Assist ■ Review ■ Approve ■ Report

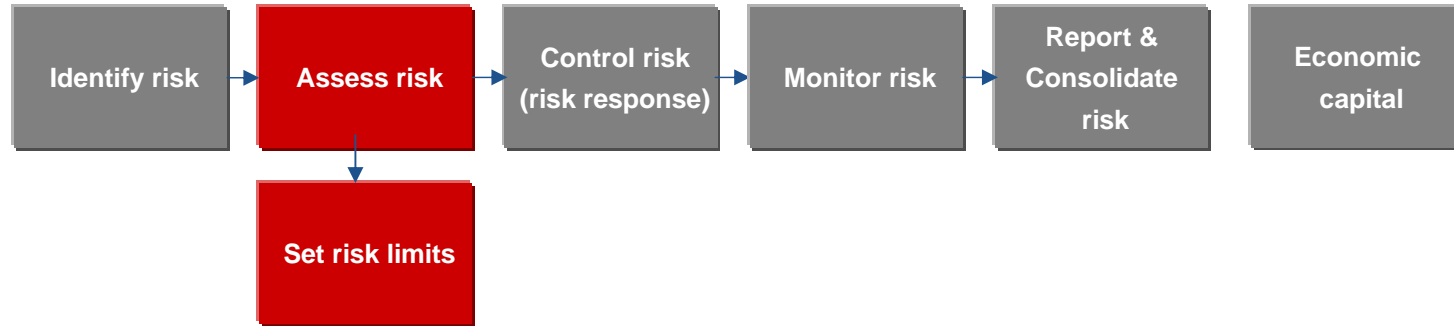
For each step in the risk management process, individual stakeholder's activities are represented



Stakeholder	Business	GM	ORC	Sub-ORC	Global WRB	Local WRB	CoC	LORM	Audit	Compliance
Process / Activity										
Risk assessment										
Provide framework					x					
Approve framework			x							
Train LORMs					x					
Set rules for RSA cycle			x							
Initiate RSA cycle				x						
Perform RSA	x									
Assist in performing RSA (if desired by business)					x		x	x		
Review RSA results								x		
Approve RSA results		x		x						
Manage exceptions				x						
Co-ordinate and plan RSA								x		
Approve planning				x						
Report on status					x				x	

Key:	■ Execute	■ Assist	■ Review	■ Approve	■ Report
-------------	--	--	--	--	--

For each step in the risk management process, individual stakeholder's activities are represented



Stakeholder	Business	GM	ORC	Sub-ORC	Global WRB	Local WRB	CoC	LORM	Audit	Compliance
Process / Activity										
Set risk limits										
Provides framework for structuring and calculating risk tolerance					x					
Approve framework			x							
Define risk tolerance limits	x									
Consolidate risk tolerance limits								x		
Review and adapt risk tolerance limits				x						
Formally review and approve risk tolerance limits; propose to EC			x							
Assist in definition and recommendation of risk limits					x					

Key:	■ Execute	■ Assist	■ Review	■ Approve	■ Report
-------------	--	--	--	--	--

For each step in the risk management process, individual stakeholder's activities are represented



Stakeholder	Business	GM	ORC	Sub-ORC	Global WRB	Local WRB	CoC	LORM	Audit	Compliance
Process / Activity										
Risk response / control										
Identify potential areas of concern	x				x			x		
Propose adequate risk response (accept or mitigate)	x									
Formulate recommendation for sub-ORC				x	x					
Approve risk response and mandate implementation			x						x	
Implement risk response	x									
Review effective implementation									x	
Report on implementation of risk response								x		

Key:	■ Execute	■ Assist	■ Review	■ Approve	■ Report
-------------	--	--	--	--	--

For each step in the risk management process, individual stakeholder's activities are represented



Stakeholder	Business	GM	ORC	Sub-ORC	Global WRB	Local WRB	CoC	LORM	Audit	Compliance
Process / Activity										
Risk monitoring										
Provide framework for identifying risk indicators and setting thresholds					Execute					
Approve framework			Approve							
Identify key risk indicators and set thresholds	Execute									
Assist in identifying key risk indicators					Assist		Assist	Assist		
Review key risk indicators								Review		
Monitor evolution of indicators	Execute				Execute			Execute		
Take action upon breach of threshold	Execute									
Review action				Assist						
Report exceptions					Report					
Manage exceptions			Execute							
Co-ordinate and plan implementation of risk indicators								Execute		
Review planning				Assist						
Report on implementation					Report			Report		

Key: ■ Execute ■ Assist ■ Review ■ Approve ■ Report

For each step in the risk management process, individual stakeholder's activities are represented

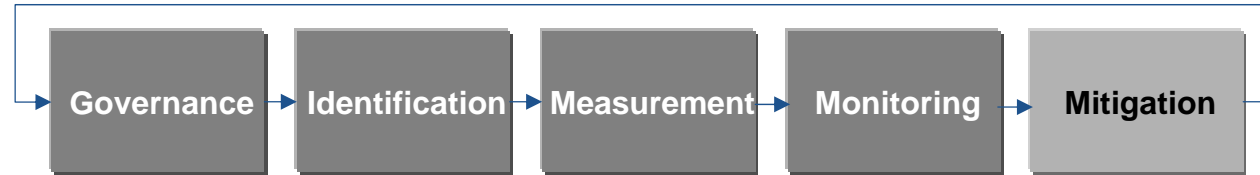


Stakeholder	Business	GM	ORC	Sub-ORC	Global WRB	Local WRB	CoC	LORM	Audit	Compliance
Process / Activity										
Risk consolidation and reporting										
Provide framework for operational risk reporting (multiple targets)					Execute					
Approve framework	Approve		Approve	Approve						
Produce operational risk reports								Execute		
Review operational risk reporting		Review	Review		Review			Review		

Key: ■ Execute ■ Assist ■ Review ■ Approve ■ Report

3. ORM Building Blocks

Operational Risk Management consists of :



Governance: Establishment of policies and the definition of the OR framework to implement these policies

Identification: Stipulation and documentation of risk exposure along process and project lines

Measurement: Qualification and quantification of risk and loss in financial value and quality

Monitoring: Identification, tracking and control of risk events and resolution thereof

Mitigation: Proactive mgmt. of risk exposure



WHAT

Process Mapping consists of a group-wide survey of processes and underlying resources that support the product offering of the financial institution, as defined by the intersection of anchor dimensions

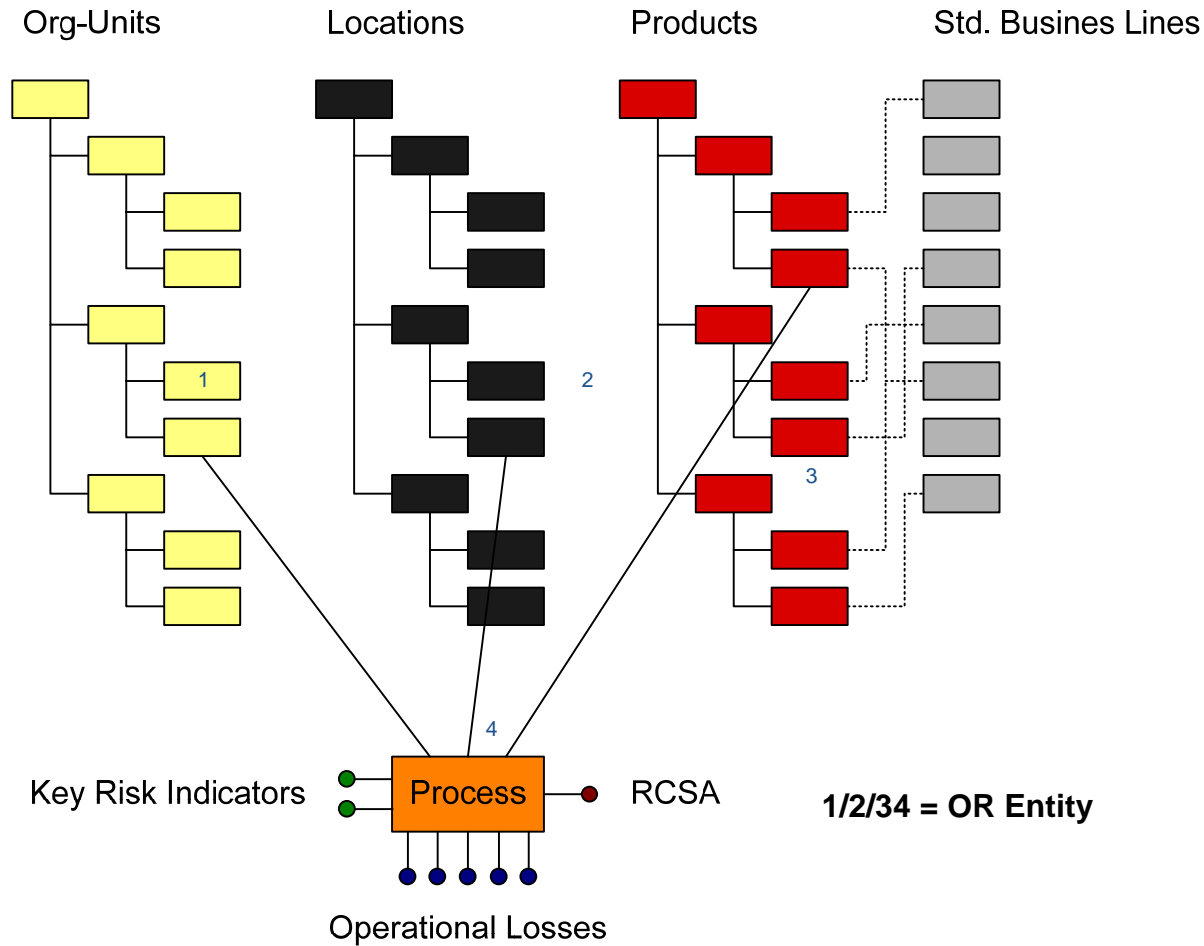
WHY

- To define Anchor Dimensions – the relevant focal points of operational risk management
- To assign operational losses
- To identify and assess risks and associated controls
- To anchor key risk indicators
- To map internal business/product lines to standard business lines (Basel II)

HOW

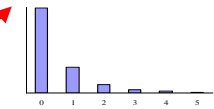
- Gather products per location and org. unit
- Gather processes, IT-systems, projects etc.
- Assign processes, IT-systems, projects etc. to products

Process mapping and anchoring Risks-Controls-Losses-Indicators





Frequency of events



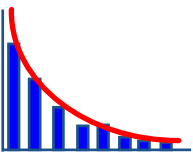
Adjusting for insurance programs



RCSA



Severity of loss

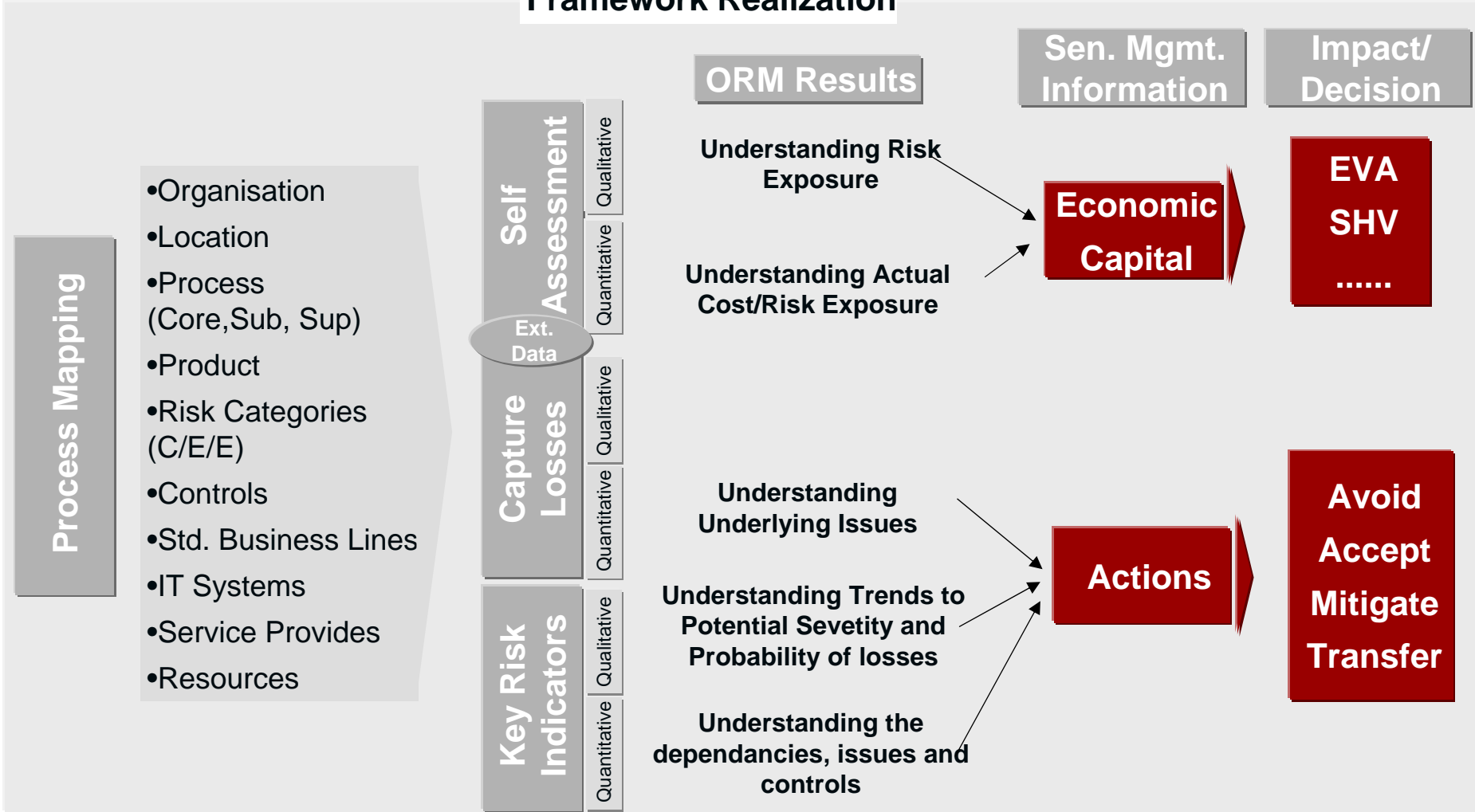


CHALLENGES TO THE LOSS DISTRIBUTIONS APPROACH

DATA CONSTRAINTS		
INTERNAL (most relevant)	CONSORTIUM (peer group)	PUBLIC LOSS DATA (use in scenario analysis)
<ul style="list-style-type: none"> 1. Timeliness and relevance to the current organization profile 2. Organizational loss experience – representative sample? 3. Data capture issues – completeness, accuracy and consistency 4. Threshold of data capture 	<ul style="list-style-type: none"> 1. Different control environments 2. Different scope and scale of business activities 3. Different levels of risk tolerance 	<p>Several issues with public loss data severely restrict, if not altogether rule out, its use for modeling purposes</p> <ul style="list-style-type: none"> 1. Reporting – large losses and certain event types more likely to be reported 2. Data capture – sources, completeness, accuracy, consistency and threshold 3. Scaling information at organization and not LoB level 4. Skewed representation of poorly controlled organizations – frequency and severity 5. Geographical location – varying degrees of legal and regulatory requirements

Results and Linkage to Performance Measures and Management

Framework Realization



4. Data Analysis - a first level example

Hypothesis: Link losses to causes, link controls to causes, identify primary causes, optimize controls, reduce losses

1. Collect loss events with identified causes over a time period as also the instances of no losses even when the cause was observed

	Number of Instances	System Down	Missing Statements	Trade Fails
Loss Incident	50	40	20	15
No Loss Incident	5,000	4,500	2,000	500
Total	5,050	4,540	2,020	515

2. Compare ratios when losses occurred when the cause was observed to the ratios when losses didn't occur even though the cause was observed

System Down		Missing Statements		Trade Fails				
Issue & Loss*	Issue & No Loss**	Issue & Loss*	Issue & No Loss**	Issue & Loss*	Issue & No Loss**			
80%	↔	90%	40%	↔	40%	30%	↔	10%

*Number of times cause was present and loss occurred/number of losses

**Number of times cause was observed/number of events without losses

3. Further, calculate the probabilistic relationships for both cases, loss and no loss across causes

	Number of Instances	System Down	Missing Statements	Trade Fails
Loss Incident	50	40	20	15
No Loss Incident	5,000	4,500	2,000	500
Total	5,050	4,540	2,020	515

	System Up	System Down	Total
Loss	10	40	50
No Loss	500	4,500	5,000
Total	510	4,540	5,050
P(L)	1.96%	0.88%	

	Statements complete	Missing Statements	Total
Loss	30	20	50
No Loss	3,000	2,000	5,000
Total	3,030	2,020	5,050
P(L)	0.99%	0.99%	

	Trade processed	Trade fails	Total
Loss	35	15	50
No Loss	4,500	500	5,000
Total	4,535	515	5,050
P(L)	0.77%	2.91%	

4. Identify all controls against such primary and secondary causes

Validate earlier assumptions – key controls, primary causes, etc.

Optimize controls against identified “true” primary causes

5. Determining Risk Appetite for an Entity

- Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that a bank is willing to retain
- Variables impacting the definition of risk appetite
 - Prioritization of risk mitigation initiatives
 - Escalation levels definition process
 - Historical data – events, assessments, KRI's and how managed
 - External drivers – peers, regulators, public
- Establishing risk appetite across levels of an enterprise – “30 mile high” to “on-the-ground”
 - Stakeholders and their requirements
 - Value drivers in meeting requirements (**limit to the scope of the risk program**)

- Derived from the value drivers of stakeholder requirements
- Value Driver – Compliance to laws and regulations
 - Zero tolerance – no breaches
 - Process of timely response
 - Derived KRI's
 - Zero tolerance – # of OR events in reporting period
 - Timely response - # of action plans overdue (<30, >30, >60 days)
 - Establishing KRI thresholds
 - Cost of compliance – how are the metric and escalation levels defined? Workshops with stakeholders – where ORM comes in
- Refining KRI thresholds
 - Examination of breach notifications, comparison against event occurrence, alignment to RCSA “quantification” metrics

- Using KRI's to identify Key Controls
 - KRI Identification must contain a common datafield with Control Identification (most often Cause)
 - Past KRI breach data, related overdue action plans
- Using KRI's to support Control Assessment ratings

Microsoft Excel - RiskLibrary Ver1 0 5 1

File Edit View Insert Format Tools Data Window Help

Type a question for help

80%

Arial

B I U

C1 OR Content Library

Business Line	Business Line Level 2	Business Line Functional Unit	Process	Process Description	Risk Category	Risk Chain	Event Description	Causes	Control Description	Key Control (Y/N)	Control Effectiveness	KRI Definition	Indicator Metric	KRI Type
4	Retail Banking	Retail Banking Sales	1 Savings, 2 Current, 3 Loans, 4 Checking, <u>Account Security - Sales</u>	Processing of Account opening forms: Collection of account opening form & relevant documents from the customer by the sales team	Unauthorized Activity / Employee misdeed	Not receiving all the information, from the customer, while opening the account.	Penalty for not following KYC: Collection of all the relevant account opening documents, from the customer, after the opening of the account. This will lead to not following the KYC norms.	1. Lack of awareness on KYC norms non-compliance. 2. Lack of time to impart training off the job with procedures etc. 3. New product policy addendum circulars not circulated to all impacted units.	1. Verify Authenticity of the financial instruments/ documents 2. Regular training programme to fulfill the staff skill set requirements.	Y	Satisfactory	Number of account opened with incomplete documentation	4	Risk Exposure
5	Trading & Sales	Operations - Front office / Treasury	All	<u>Information Security</u> Theft of Information:	System security breach	No policies / procedures for better access controls.	Inadequate control on staff terminal: Inadequate control on staff terminal may result in loss of critical customer information, fraud and infringement of regulatory requirement of confidentiality.	1. No Role Based Access controls/review. 2. Lack of time to impart training to the staff. 3. Negligence to follow up and adopt checklist.	1. PC access protection procedures in place. 2. Anti-virus software installed in all the PCs and updated periodically. 3. A password protected screen saver will be activated at a maximum of 15 min activity. 4. Any change of employee status, like transfer, resignation, the profile will be removed with in 24 hours from the system. 5. It is mandatory for all staff to attend the training on Information security.	N	Satisfactory	Number of Internal fraud occurred due to information security breach.	2	Risk Severity

Questions



Pat Medapa

Director, Oprisk and GRC
Practice, Risk Tech

India

Tel:+91 80 2213 1820

Mobile: +91 99875 11538

E-mail: patm@risk-technology.com

Background

- Pat has extensive ORM domain and solution development and implementation experience.
- He has served as a key consultant in AMA capital estimation projects at banks in the US, France, Germany and Australia
- He has served as the functional lead in product development and pre sales at a leading operational risk management solution provider
- He holds an MBA (Fin) and is a science graduate

Role / Skills

- SME – Operational Risk Management
- ORM solution selection and implementation
- ORM Process Consulting

Key Risk and Technology Experience

- He has been involved in the Operational Risk Management (ORM) field for over twelve years and has worked at consulting and technology solution providers in the US and India
- He has served as the Functional lead involved in the acquisition, transition and final overlay of an ORM point solution onto an enhanced technical and functional platform at a leading ORM solution provider
- He has served as an engagement manager and a key implementation resource while working at two ORM technology providers during the course of eight implementation projects in North and South America. Notably, he successfully delivered the Business Specifications covering the requirements of an estimated 50,000+ user base during the implementation of a Risk and Control Self assessment module at a large global bank
- He has hired and trained resources and developed a Knowledge Base that were the reference source and foundation for ORM resources at a leading technology provider
- He has managed the outsourced development of two ORM solutions, OpRisk Monitor and OpRisk VaR, the precursors of the current SAS ORM technology offering
- He has served as a key project resource, including project manager, during his stint at a Big Four consulting firm delivering consulting and LDA methodology under the AMA approach to capital estimation at banks in the US, France, Australia and Germany
- He has built and maintained internal and external operational risk event databases at the some of the firms he has worked at over the course of his career
- He was part of the team that pioneered ORM at a leading Wall Street investment bank
- He has presented at various conferences across the globe, participated in round table discussions on ORM and authored several articles
- He has worked at the following banks in the following roles
 - Part of a three member team that delivered capital estimation consulting projects at banks that include Citigroup, JP Morgan Chase, National Australia Bank, Bayersiche Landesbank and Deutsche Bank
 - As engagement manager of solution implementation projects at various regional North American banks such as Banque National du Canada, Capital One and Old National
 - Most recently he drove a successful solution implementation at Interbank in Peru as also played a key functional role in the phased solution implementation of an RCSA module across Citigroup.