Operational Risk Management Conference

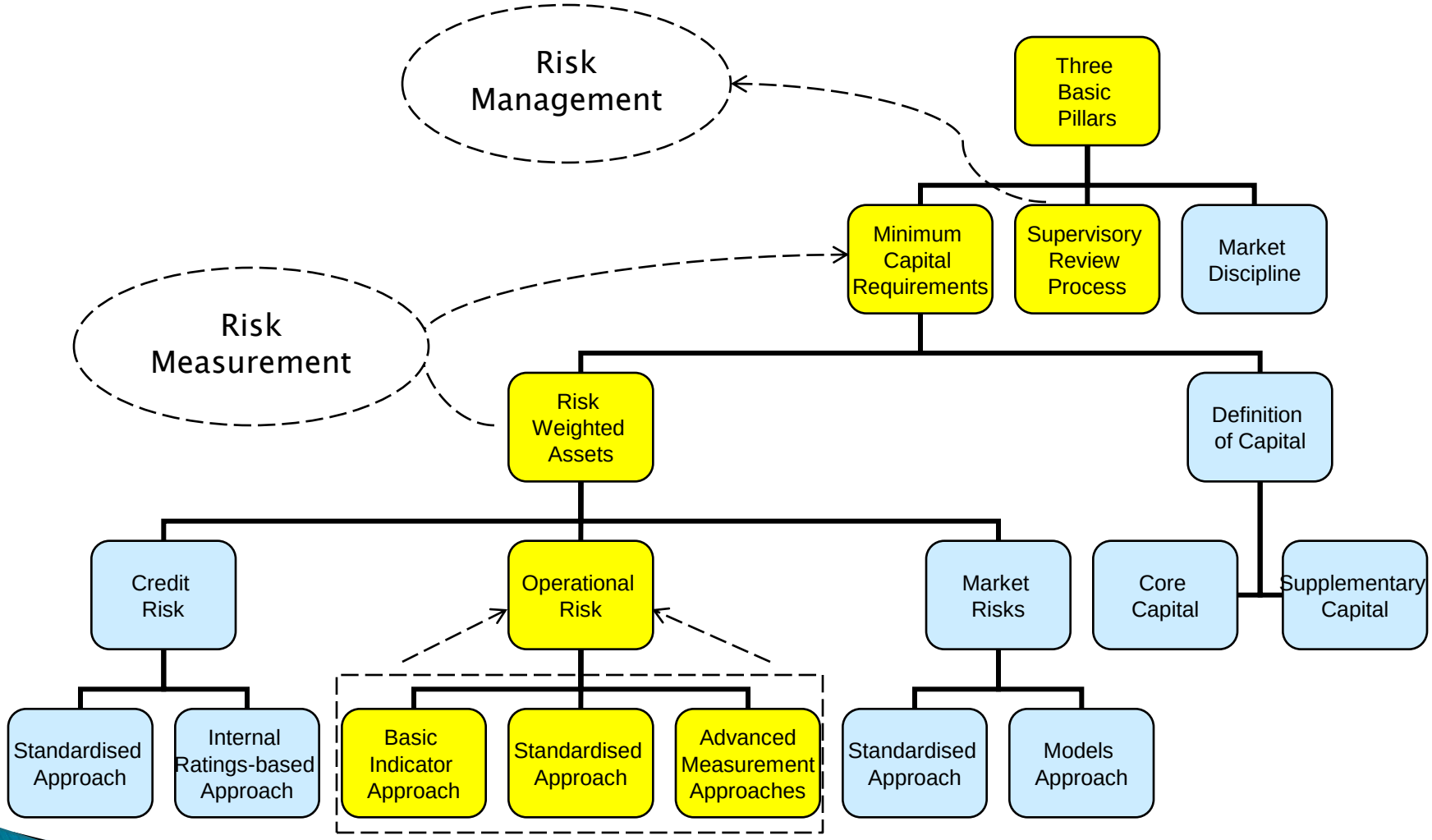
State Bank of Pakistan

February 8th, 2013

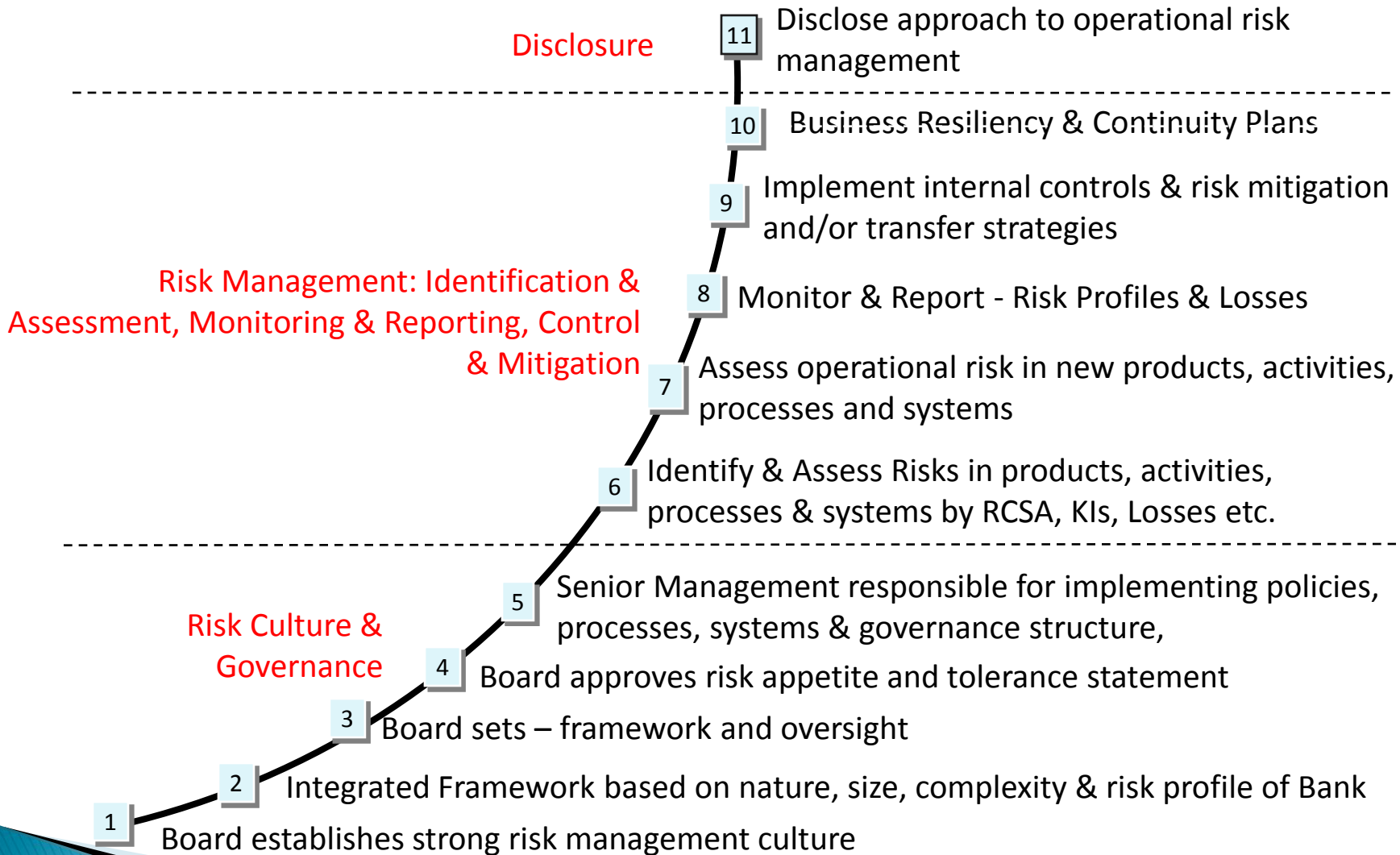
Topics for Discussion

- Basel Overview
- Sound Practices for Operational Risk
- Operational Risk Framework
  - Governance
  - Tools
- Operational Risk Measurement

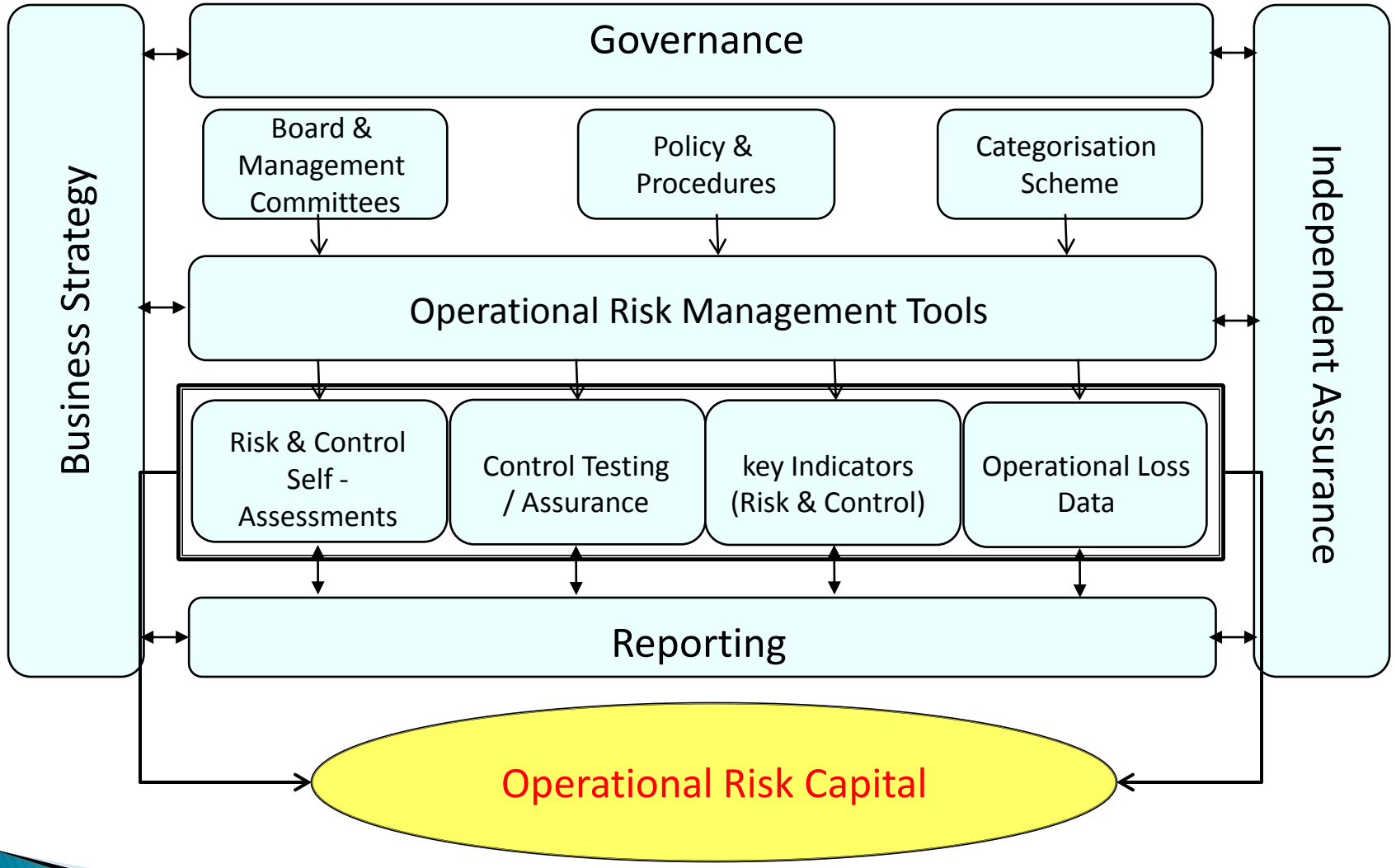
Basel II – Basic Structure



Operational Risk Management Principles



Operational Risk Management Framework



Governance – Committee Structure

Board Risk Committee (s)

Executive Management Committee/
Management Risk Committee

- Operational Risk Committee
- Information Security Committee
- Fraud Management Committee
- New Products Committee
- Compliance Committee

- Various Governance structures – no right or wrong
- Specific to the requirements of the organization – what works best?
- Maturity with time

Governance – Policy & Procedures

- Policy ideally should focus on WHAT
- Procedures should define HOW

Definition & Responsibilities

- Definition of Operational Risk
- Roles & Responsibilities of Stakeholders in the ORM Process

Event Categories (7)

- Internal Fraud
- External Fraud
- Employment Practices & Workplace Safety
- Client, Products & Business Practices
- Damage to Physical Assets
- Business Disruption & System Failures
- Execution, Delivery & Process Management

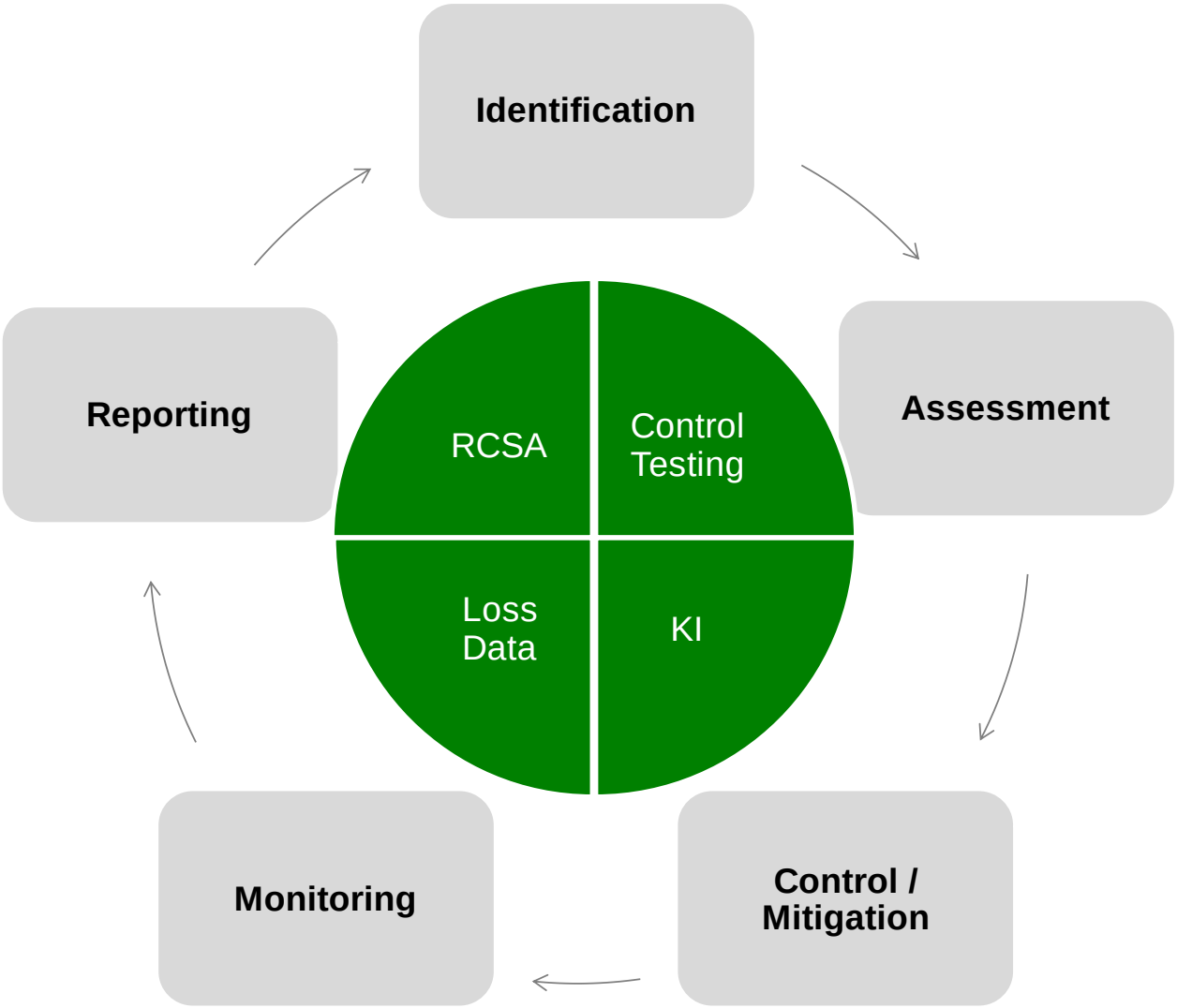
Causal Factors (4)

- People Inadequacies/Failure
- Process Inadequacies/Failure
- Systems Inadequacies/Failure
- External Events

Risk Management Philosophy

1st line of Defence	*2nd line of Defence*	*3rd line of Defence*
Business Management	Operational Risk Management	Group Audit

Governance – Policy & Procedures



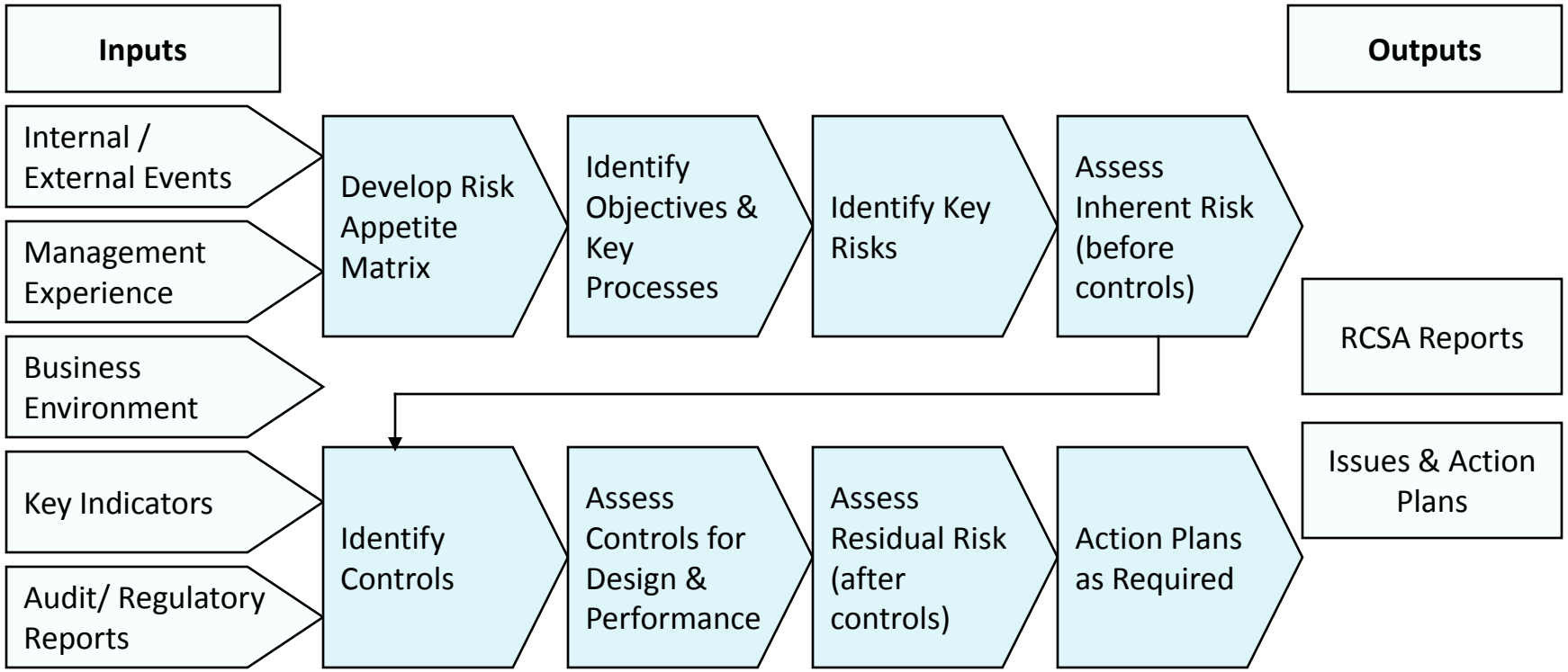
Operational Risk Management Tools

Tool	Approach	Frequency
Risk & Control Self – Assessments	• Workshop based. Assess risks & controls • Predefined risk assessment matrix • Action plans	Half Yearly / Yearly or Major Change
Key Indicators	• Identification of risk points in a process • Linked to risks & controls • Monitored against benchmarks	Monitor Each Month
Operational Loss Events	• Reportable events & amounts • Predefined categorization scheme • Escalation timelines based on amount • Lessons learnt	Reporting Based on Amount
Control Assurance / Testing	• Regular testing of key controls • Helps strengthen control environment	Quarterly / Half Yearly
Change / Outsourcing Risk Assessment	• Review new products, systems, processes • Mandatory input • Conditions monitored	As & When Introduced

Risk & Control Self – Assessment (RCSA)

- Is a systematic process for identification & assessment of key operational risks that can impact the achievement of business objectives.
- Provides a narrative/outline of risks within the business unit & controls mitigating the risks.
- Highlights areas for improvement & management focus / attention
- Benefits include:
  - Progressive risk management with tangible identification and assessment of operational risks
  - Provides visibility / transparency of operational risks that Business Units are taking and how they are managing them
- Concerns
  - Self Assessment carried out by business units – tendency to play down risk exposures & elevate control environment

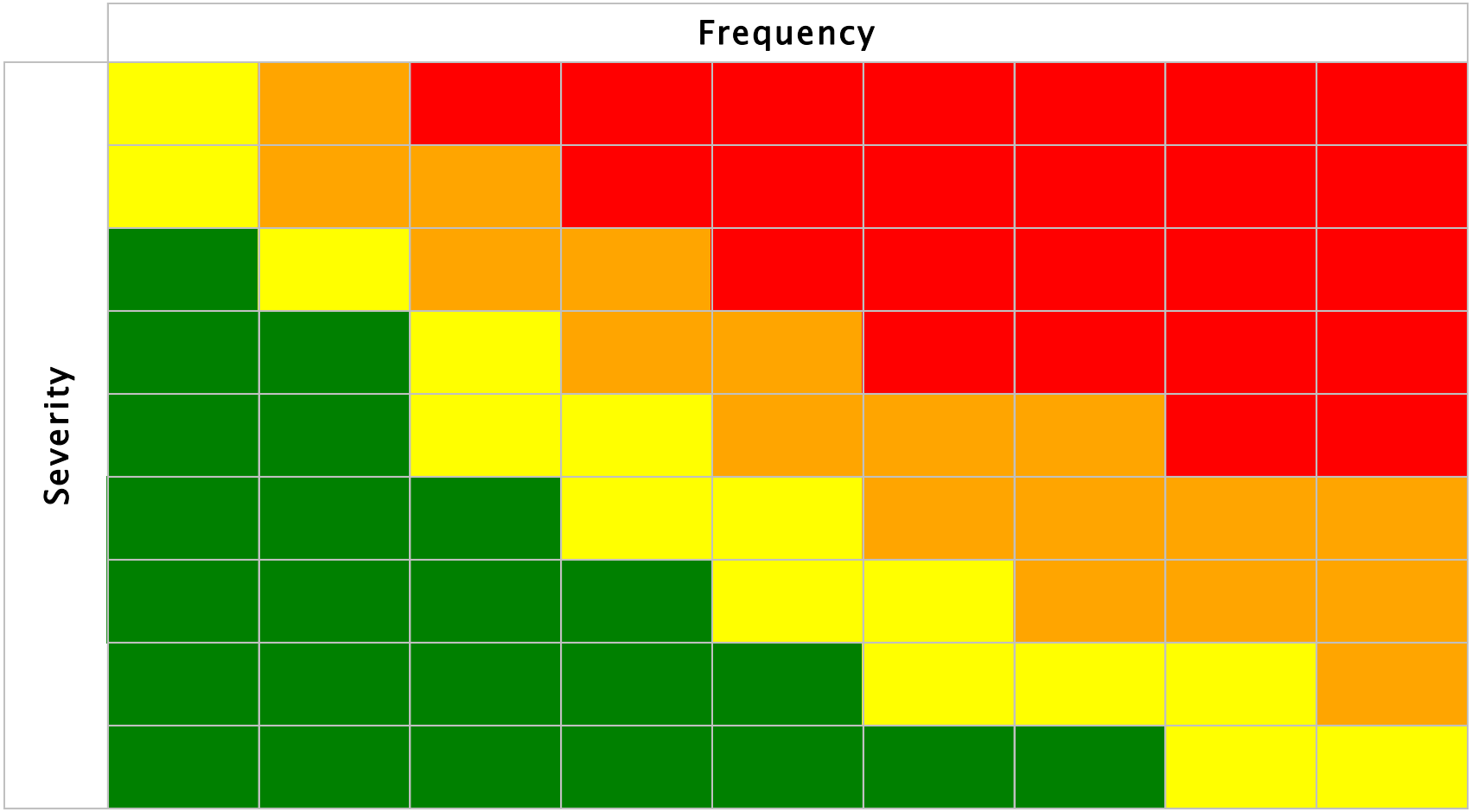
Risk & Control Self – Assessment (RCSA)



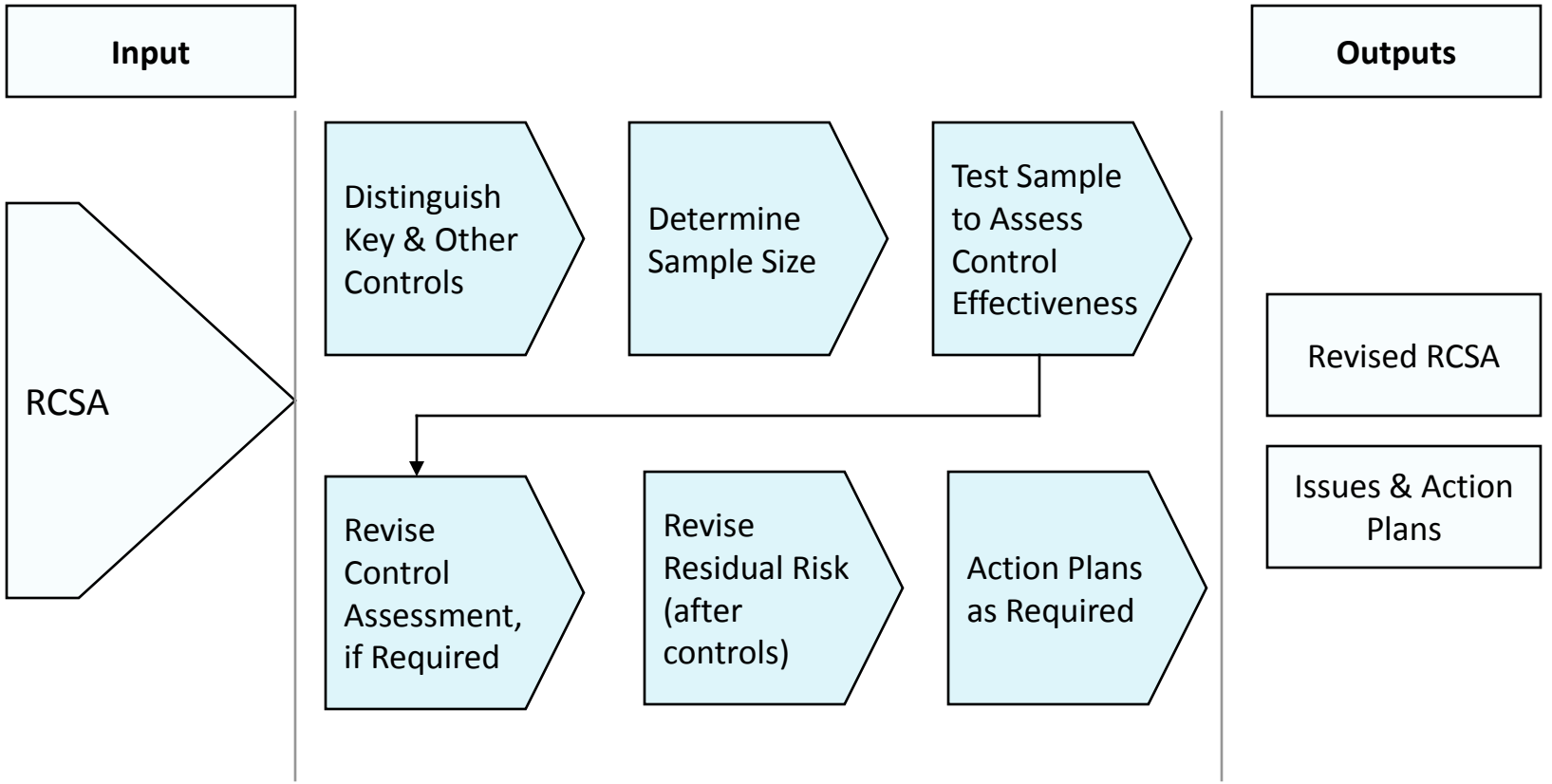
- Subject to periodic review and dynamic maintenance i.e. to be updated for any material changes in the business
- Controls validation/assessment to be done more frequently

Risk & Control Self – Assessment (RCSA)

Sample Heat Map



Control Assurance /Testing



- More frequent testing of key controls.
- Helps converting a subjective assessment of controls into an objective one.

RCSA / Control Testing - Challenges

- Differentiation between risks and lack of controls
- Determining the appropriate level of granularity when capturing risks
- Risk Ranking – High /Medium /Low or a Frequency & Severity Matrix
- Risk Materiality – a material risk for one unit may not be a material risk for another unit or the Bank
- Some risks are difficult to tie to a frequency & severity scale
- Control Testing – stepping on Internal Audit's toes

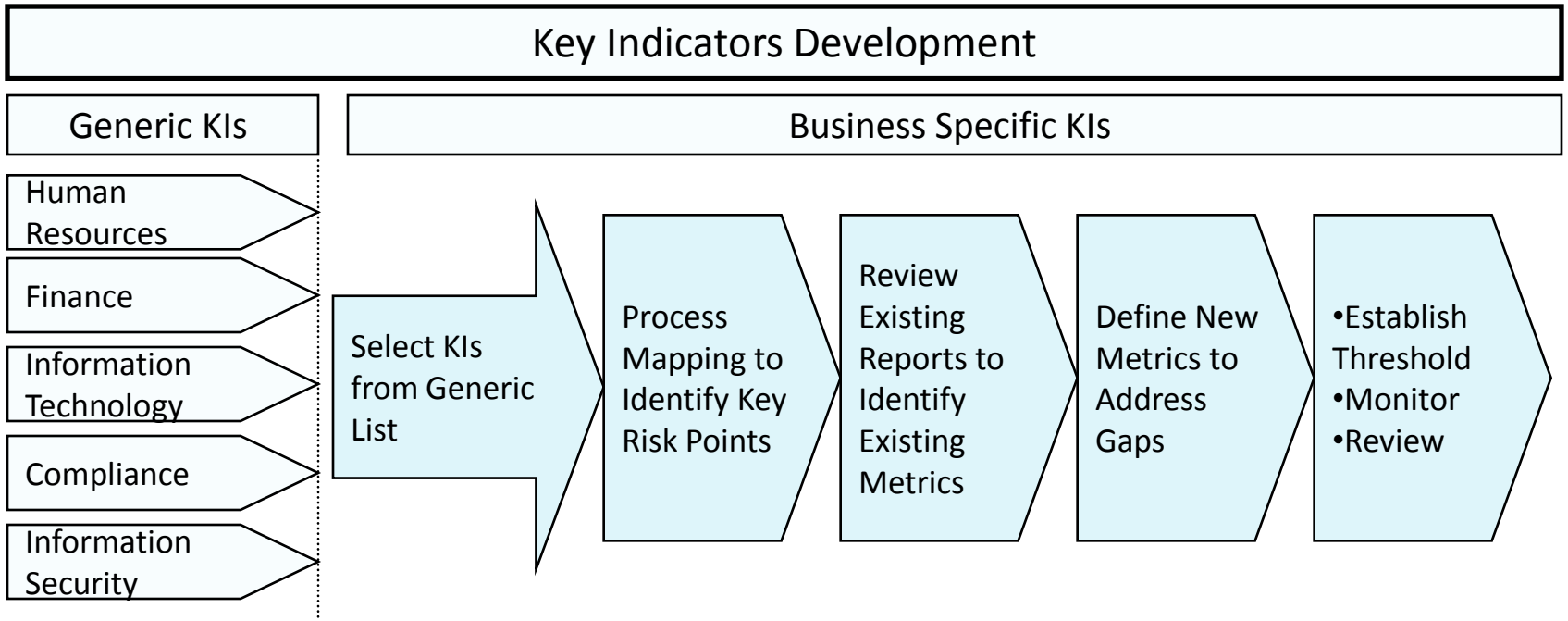
Suggestions:

- Follow Basel Event Categorization Scheme
- Create a Risk Register and a Control Library
- Use a Frequency & Severity Based Matrix with Different Business Thresholds

Key Indicators (KI)

- KIs are early warning signals of an increased risk of a future loss. E.g.:
  - Employee Turnover Rate
  - Critical Systems Availability (system downtime)
  - Processing Error Rate
- Indicate changes in the operational risk, or the potential for loss in a process.
- Provide objective information on emerging operational risk issues & trends.
- Could provide insights into correlations between business / control environment changes and operational losses.
- Generally there are two types of KIs:
  - Generic: Applicable across the organization, e.g. Employee Turnover Rate
  - Business Specific: Applicable to a specific business, e.g. Late Settled Trades

Key Indicators (KI)



Challenges:

- Identifying "Key" while ensuring reasonable coverage
- Data availability issues for new indicators
- Establishing Thresholds
- Benchmarking

Suggestions:

- Develop, monitor, review and refine key indicators and thresholds overtime

Key Indicators (KI)

Sample Key Indicator Report

			Actual Data			Thresholds		
Status	Trend	Key Indicator Name	Oct	Nov	Dec	Yellow	Amber	Red
●	↑	Staff Turnover (Annualized)				10 %	15 %	20 %
●	↑	Employees Leaving Within First 2 Years				2 %	3 %	5 %
●	↓	Sick Days Reported				250	500	750
●	←→	Average No. of Employees Per Manager				10	20	30
●	↑	Percentage of Employees Who Attended Training				15 %	10 %	5 %
●	←→	Overtime Per Eligible Employee in Hours				2	5	8
●	←→	Employees Aged 58 and Above				25	50	75
●	↓	Staff without 2 Weeks Consecutive Leave				10 %	15 %	20 %

Notes:

- Reporting should meet the organization's requirements
- Report shows, latest status for each KI, trend compared to last month, two months history and thresholds.

Operational Loss Data

Operational Loss is an out-of-pocket or other real, objectively measurable, economic loss that results from an operational failure event. For a loss to occur, an ***operational failure event must occur first***. Loss is the resultant financial or monetary loss.

Typical Inclusions in Determining Loss
Fees, fines and penalties paid by the Bank
Legal Costs of external counsel / lawyers
Payments or other compensation paid to customers or third parties because of Bank's failure or Bank's vendor's failure
Payments made to incorrect third parties (recoveries will be measured separately)
Lost interest or float income from incorrect payments made or fees billed to third parties
Reduction in value of financial assets because of a failure event
Expense above expected or budgeted costs to fix an operational failure
Value of insurance claims for which we cannot be reimbursed
Hardware costs to fix a system or process that failed
Payments to third parties to remediate a failure
Waiver of fees or other costs incurred following a disaster

Operational Loss Data

Exclusions
Expenses that are expected and within the budget
Costs to redesign a system or process to prevent future failures. These are considered investments
Estimates of “soft” costs from damage to reputation or costs to re-build reputation
Costs associated with a decision to waive requirements or business terms if the waivers were unrelated to an operational failure or external event, and were properly executed
Credit or market risk losses unrelated to an operational failure
Estimates of market share losses and resulting foregone profits because of an operational failure

Outcomes of a Failure Event :

1. Actual Loss
2. Near Miss
3. Operational Gain
4. Potential Loss

Operational Loss Data

Sample Loss Record

Date of Loss	Date of Discovery	Date of Accounting
Brief Description	Risk Event Category	Causal Category
Bank's Reporting Unit	Bank's Effected Unit	Basel Business Line
Gross Loss Amount	Insurance Recovery	Other Recovery
Net Loss Amount		

Operational Loss Data

Sample Escalation / Reporting

Escalation Matrix				
Amount (PKRs)	Reporting By Department (To & Within Number of Business Days)			
	Business Operational Risk	Group Head	Group Operational Risk	Senior Management
> 1000,000	Immediate	Immediate	Immediate	Immediate
500,001 – 1,000,000	Immediate	Immediate	3 days	3 days
250,001 – 500,000	Immediate	3 days	5 days	5 days
100,001 – 250,000	Immediate	5 days	10 days	10 days
< 100,000	Monthly Report	Monthly Report	Monthly Report	Monthly Report

Operational Loss Data - Challenges

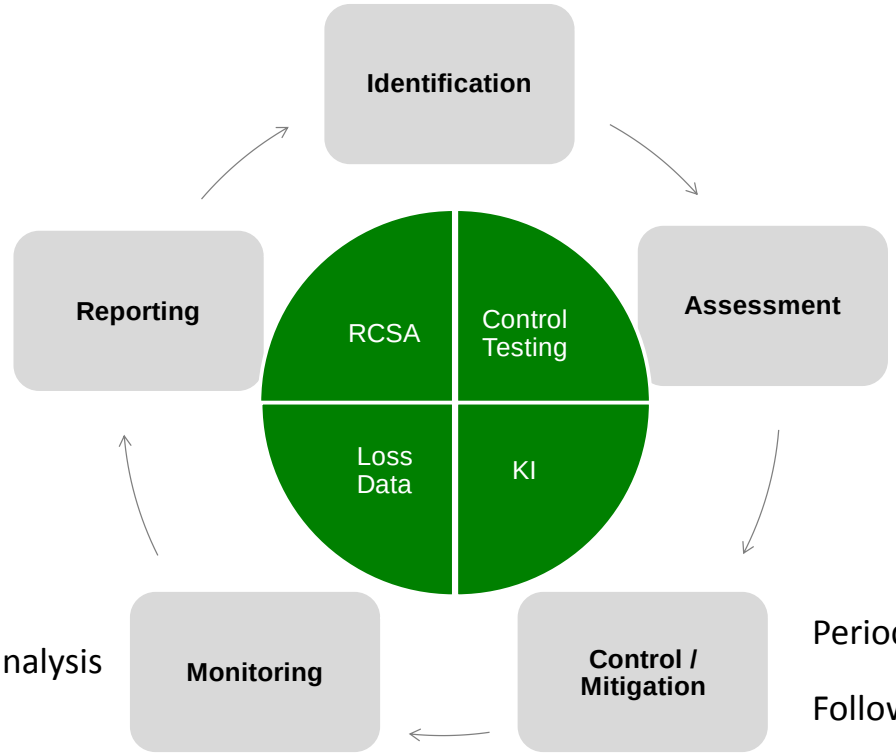
- Cost of doing business mentality
- Fear of being penalized
- Recognition (booking) and reconciliation
- When does a Suspense accounts item become a loss
- Potential Loss vs. Actual Loss
- Attribution of losses in centralized functions
- Ensuring completeness and accuracy of data
- Boundary issues – Credit and operational losses

Operational Risk Management Process

RCSA/KI/Loss data

Int / Ext Audit reports

Results of Control Testing



Inherent & residual risk

Control design/ performance

Risk Appetite

Historical Loss data

Periodic Control Testing

Follow up on Action Plans

RCSA Reviews

KI / Loss data analysis

KI monitoring

Action plans

Top 10 risks

KI breaches

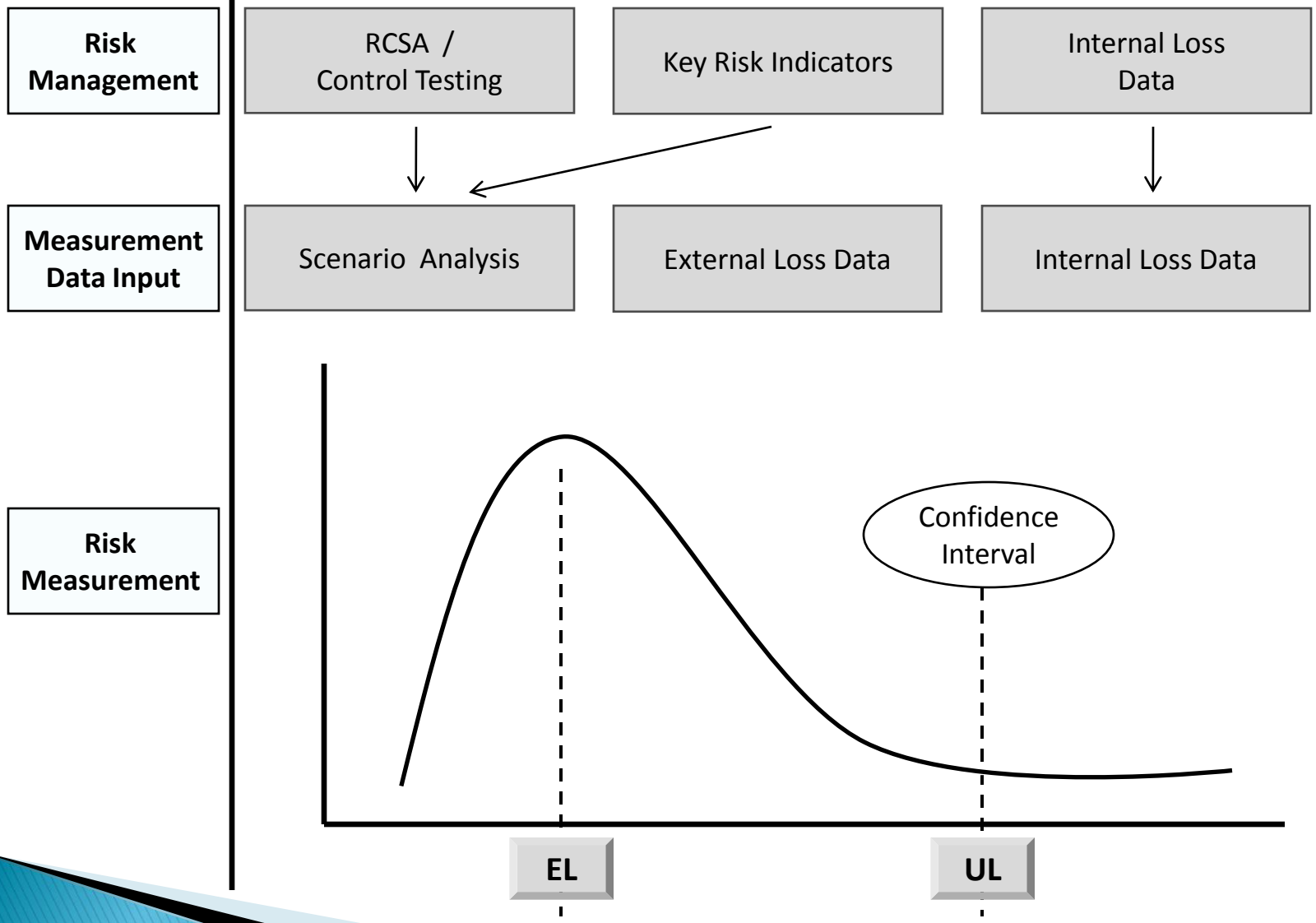
Loss data analysis

Operational Risk Measurement

Basic Indicator Approach (BIA)	The Standardized Approach (TSA)	Advanced Measurement Approaches (AMA)
➢ Capital = 15% of average gross income over last 3 years ➢ Years for which gross income is negative or zero are to be excluded ➢ Banks are to comply with Sound Operational Risk Management Practices	➢ Bank's activities are divided into 8 business lines ➢ Beta factor is assigned to each business line ➢ Capital = average gross income over last 3 years for each business line X assigned beta factor ➢ Years for which gross income is negative or zero are to be excluded ➢ Bank Capital = Sum of business line capital numbers ➢ Compliance with SPOR and BIS Qualifying Criteria	➢ Bank's activities are divided into 8 business lines ➢ Operational losses to be collected according to a "Loss Event Classification Scheme" ➢ Framework must include: - Internal /external loss data & scenario analysis - Business environment & Internal control factors ➢ Capital is measure generated by the bank's internal risk measurement system ➢ Subject to strict additional qualifying criteria and regulatory approval

Increasing Sophistication

Operational Risk Measurement - Aspiration



Final Thoughts Suggestions

- Develop, implement and refine along the way - perfecting the framework will delay implementation
- Establishing an operational risk data consortium will significantly speed up the maturity and value

Thank You