Operational Risk & Basel II

Arsalan Ahmed Qureshi
Manager Operational Risk

Agenda

- Defining and Understanding Oprisk
- Why Oprisk Management
- Evolution of Basel II
- Sound Practices for Management of Oprisk
- Basel II – SBP Guidelines
- Operational Risk Loss Data Issues
- Managing the Oprisk – The Framework
- Standard Based Approach to Oprisk

Defining & Understanding Operational Risk

"Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events."

Basel Committee on Banking Supervision

Defining & Understanding Operational Risk

Operational risk deals mainly with tail events rather than central projections or tendencies, reflecting aberrant rather than normal behavior and situations. Thus, the exposure to operational risk is less predictable and even harder to model

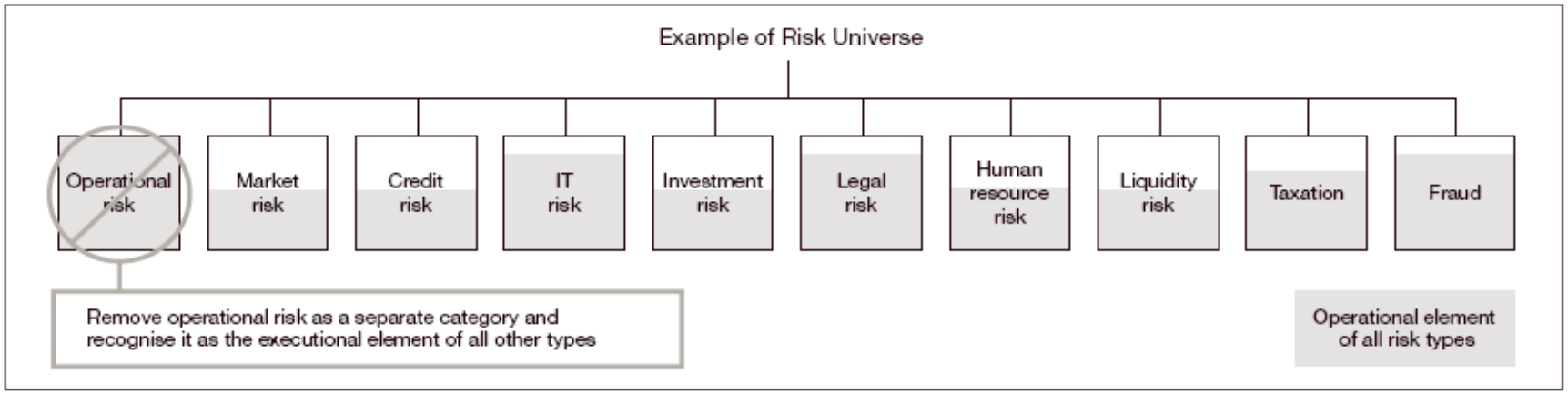
Defining & Understanding Operational Risk

Integrated Operaional Risk Management:

Operational risk exists in every part of the financial institution and for that reason alone, ORM must be conducted within each line of business,

business unit, and functional department

Figure 1 – Embedding operational risk



Defining & Understanding Operational Risk

- **Process Risk:** Risks related to the execution and maintenance of transactions, and the various aspects of running a business, including products and services.

- **People Risk:** The risk of a loss intentionally or unintentionally caused by an employee i.e. employee error, employee misdeeds— or involving employees, such as in the area of employment disputes. This risk class covers internal organizational problems and losses.

- **System Risk:** The risk of loss caused by a piracy, theft, failure, breakdown or other disruption in technology, data or information; also includes technology that fails to meet business needs.

- **External Risk:** The risk of loss arises due to damage of physical property / assets from the natural or non–natural causes. This category also includes the risk presented by actions of external parties, such as the perpetration of fraud, or in the case of regulators, the execution of change that would alter the firm's ability to continue operating in certain markets

Defining & Understanding Operational Risk

Business Area	Potential Risks
Process	• Breach of mandate • Incorrect/untimely transaction capture, execution, and settlement • Loss of client assets • Mis-pricing • Incorrect asset allocation • Compliance issues • Corporate action errors • Stock lending errors • Accounting and taxation errors • Inadequate record-keeping • Subscription and redemption errors

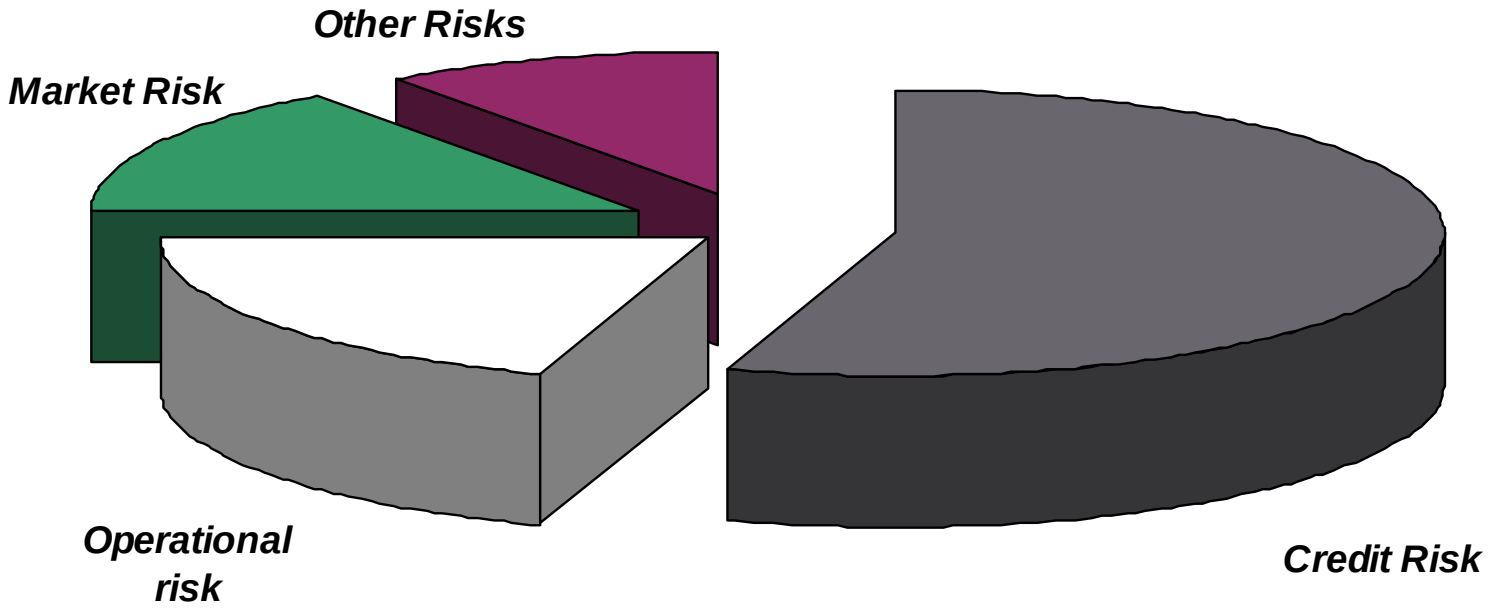
Defining & Understanding Operational Risk

Business Area	Potential Risks
People	• Unauthorized trading • Insider dealing • Fraud • Employee illness and injury • Discrimination claims • Compensation, benefit, and termination issues • Problems recruiting or retaining staff • Organized labor activity • Other legal issues

Defining & Understanding Operational Risk

Business Area	Potential Risks
Systems	• Hardware and/or software failure • Unavailability and questionable integrity of data • Unauthorized access to information and systems security • Telecommunications failure • Utility outage • Computer hacking or viruses
External Events	• Operational failure at suppliers or outsourced operations • Fire or natural disaster • Terrorism • Vandalism, theft, robbery

Defining & Understanding Operational Risk



Defining & Understanding Operational Risk

"More than 80% of our Credit risk is really just Operational risk."

Senior Risk Officer,
Large German Bank

Why Operational Risk Management

Why Operational Risk Management

- Recognition of Oprisk important because reflects changes in financial institutions' risk profile inherent in developments such as:

- use of highly automated technology
- growth of e-banking
- large scale Merger & Acquisitions that test viability of newly integrated systems
- emergence of banks as very large service providers
- increased prevalence of outsourcing
- enhanced use of new risk mitigants for credit and market risks, but potentially creating increased operational risk

Why Operational Risk Management

- It allows banks to identify source of operational losses and take mitigating actions
- It allows banks to identify operational loss outcomes that they have exposure to, but have yet to experience
- Provides a framework for modeling extreme events.
  - "Scenario Analyses" of low frequency, high severity events.
- Help incorporate the quantification of "risk reduction" into the decision making process

Why Operational Risk Management

- A lower regulatory capital requirement
- Reduced losses (due to speed of response etc)
- Lower operating costs
- Lower insurance premia
- Lower cost of financing
- Improved share price
- Stability of earnings
- Enhanced value for stakeholders

Basel II – Evolution of Operational Risk

Basel II – Evolution of Ops Risk

- **1988 Capital Accord**
  - Too simplistic
  - Subject to manipulations
  - Encouraged more risk taking
  - Leading banks, using sophisticated models realized that they were 'over capitalized' and lobbied for a more risk sensitive capital framework.

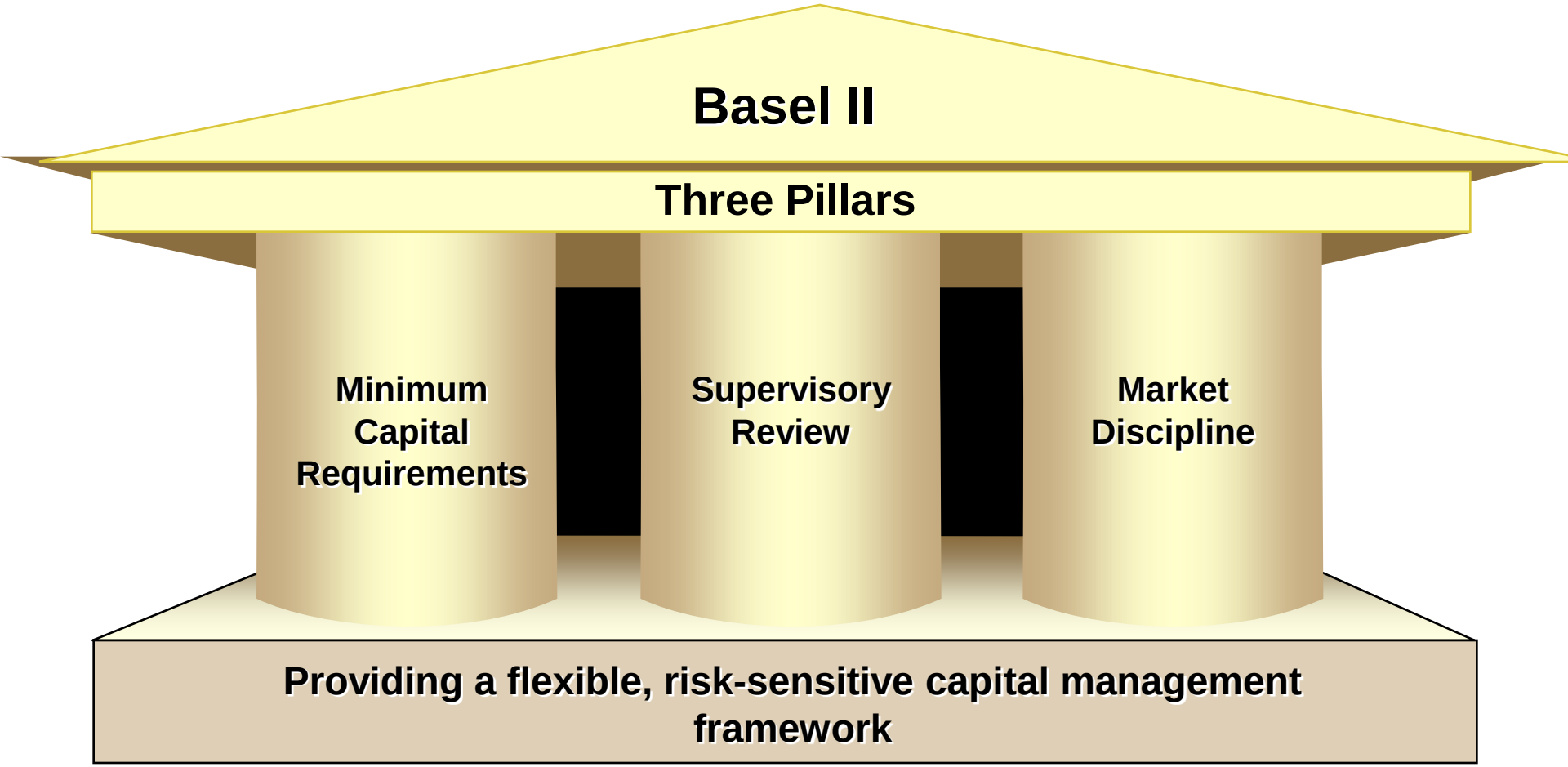
Basel II – Evolution of Ops Risk

- **The New Accord**

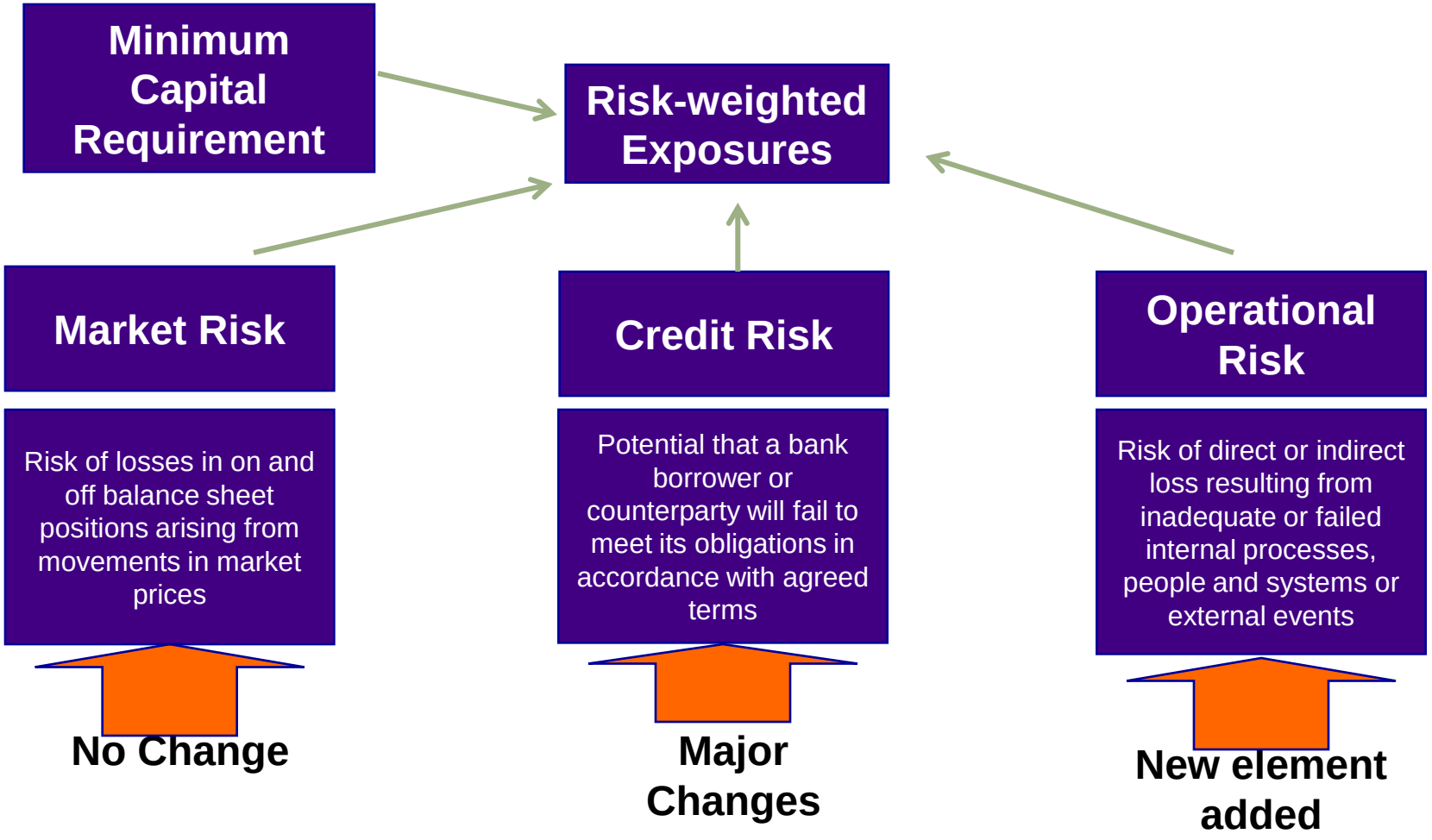
  Basel II is based on the fundamental principle that risk capital should be based on level of risk (i.e., risk sensitive).

  - Incentive: Requiring banks to hold capital based on their actual level of risk. Would give banks an incentive to reduce their level of risk

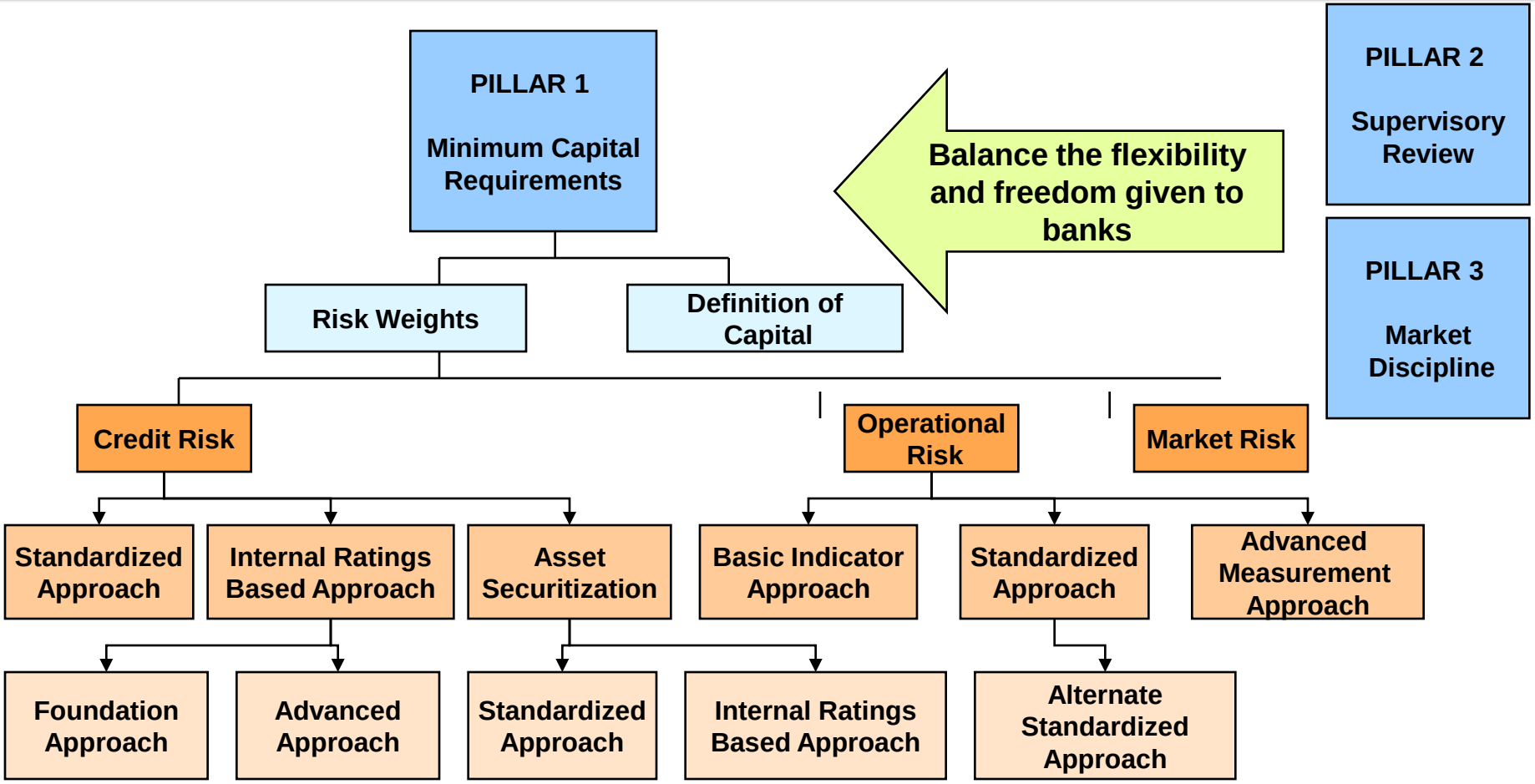
Basel II – Evolution of Ops Risk



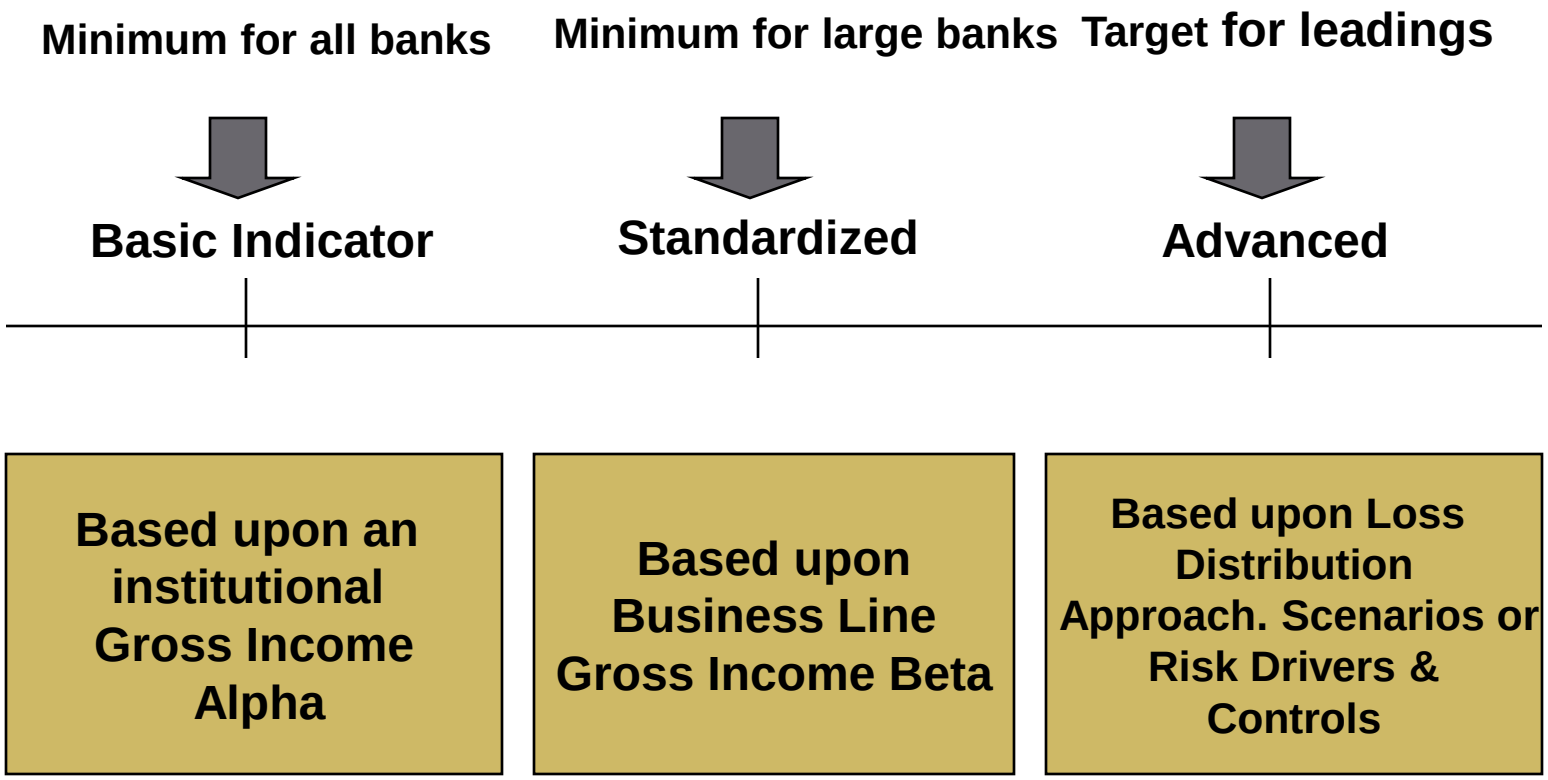
Basel II – Evolution of Ops Risk



Basel II – Evolution of Ops Risk



Basel II – Evolution of Ops Risk



But also requires adherence to a set of "Sound Practices"

Basel II – Evolution of Ops Risk

Approach	Basic Indicator Approach	Standardized Approach*	Advanced Measurement Approaches (AMA)
Calculation of Capital Charge	• Average of gross income over three years as indicator • Capital charge equals 15 percent of that indicator	• Average gross income over three years per regulatory business line as indicator • Depending on business line, 12 percent, 15 percent, or 18 percent of that indicator as capital charge • Total capital charge equals sum of charge per business line	• Capital charge equals internally generated measure based on: – Internal loss data – External loss data – Scenario analysis – Business environment and internal control factors • Recognition of risk mitigation (up to 20 percent possible)

Basel II – Evolution of Ops Risk

Approach	Basic Indicator Approach	Standardized Approach*	Advanced Measurement Approaches (AMA)
Qualifying Criteria Compliance with the Basel Committee's "Sound Practices for the Management and Supervision of Operational Risk" recommended for all approaches.	• No specific criteria	• Active involvement of board of directors and senior management • Existence of OpRisk management function and independence of that function • Sound OpRisk management system • Systematic tracking of loss data	• Same as Standardized, plus: • Measurement integrated in day-to-day risk management • Review of management and measurement processes by internal/ external audit • Numerous quantitative standards – in particular, three to five years of historic loss data

Sound Practices for the Management & Supervision of Operational Risk

Ops Risk best Practices

- Basel Committee on Banking Supervision – Dec 2001 is organized around the following key areas:

(a) Developing an appropriate risk management environment;
(b) Risk Management: identification, measurement, monitoring and control;
(c) The role of supervisors and
(d) The role of disclosure.

Ops Risk best Practices

- Developing an Appropriate Risk Management Environment
  - Principle 01: Approved Oprisk Management framework by BoD and BoD's should be aware of the major aspects of the bank's operational risk
  - Principle 02: Oprisk department should be independent from internal audit
  - Principle 03: Senior management should have responsibilities of implementing Oprisk management framework approved by BoDs and it should be disseminate to all the staff.

    Senior management is responsible for developing policies, process and procedures for managing operational risk in the bank's entire material product, activities, process and systems.

Ops Risk best Practices

- **Risk Management: identification, measurement, monitoring and control**
  - Principle 04: Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.
  - Principle 05: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.
  - Principle 06: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.
  - Principle 07: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Ops Risk best Practices

- **Role of Supervisors**
  - Principle 08: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.
  - Principle 09: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.
- **Role of Disclosure**
  - Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

Operational Risk – *Loss Data Issues*

Basel II

- **Internal Loss Data tracking**
  - Internal loss data is most relevant when it is clearly linked to the institution's current business activities, technological processes and risk management procedures.
  - Assessing the on-going relevance of historical loss data, including those situations in which judgment overrides, scaling, or other adjustments may be used
  - Minimum five-year observation period of internal loss data. When the bank first moves to the AMA, a three-year historical data window is acceptable.

Basel II

- **Internal Loss Data tracking**
  - Bank must be able to map its historical internal loss data into the relevant level 1 supervisory categories.
  - The internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems and geographic locations.
  - A bank must have an appropriate *de minimis* gross loss threshold for internal loss data collection
  - Aside from information on gross loss amounts, a bank should collect information about the date of the event, any recoveries of gross loss amounts, as well as some descriptive information about the drivers or causes of the loss event.

Basel II

- **Internal Loss Data tracking**
  - Treatment of Operational risk losses that are related to credit risk – Collaterals.
  - Operational risk losses that are related to market risk are treated as operational risk for the purposes of calculating minimum regulatory capital and will therefore be subject to the operational risk capital charge.

Basel II

- **External Data**
  - The operational risk measurement system of bank must use relevant external data (either public data and/or pooled industry data), especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses.
  - External data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events to assess the relevance of the loss event for other banks
  - Must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments etc.

Issues in collection of Loss Data

- **Fundamental problem**

"In the field of operational risk management, it's hard to find good data. Internal loss data seem to be insufficient and external loss data are affected by reporting biases and numerous idiosyncratic factors"

Data Collection

- "Currently, there is not sufficient data at the industry level or in a sufficient range of individual institutions to calibrate the capital under this (Internal Measurement) approach. The Committee will have to be satisfied that a critical mass of institutions have been able individually and at an industry level to assemble adequate data over a number of years to make the approach workable."

(p8 paragraph 31 OR Supporting Document of Basle Committee)

Data Collection *(continued)*

- Requires more work
- Standards require definition
- Internal Measurement Approach will not be available without data – *but how much data are the regulators expecting (they tend to refer to years rather than no. of data points)?*
- Integrity of data has to be established
- Systems enhancement / development needed to collect data and build a database
- Internal data will need to be supplemented by external data
- Industry data needs to be pooled in codified, centralised operational risk databases
- All of the above will take significant resources and time for the industry to do well

Issues in collection of Loss Data

- **Major issues with loss data**
  - Most institutions don't have a lot of internal loss data.
  - Many operational loss data sets have very "long tails"
  - In summary, internal data is insufficient to be used in a meaningful manner.
  - To address this problem, many institutions have chosen to supplement their internal loss data with external loss data

Issues in collection of Loss Data

- **Problems with external loss data-Pooled**
  - Idiosyncratic factors
    - size
    - controls
    - culture
    - business processes
    - legal
    - environment and
    - geographic location

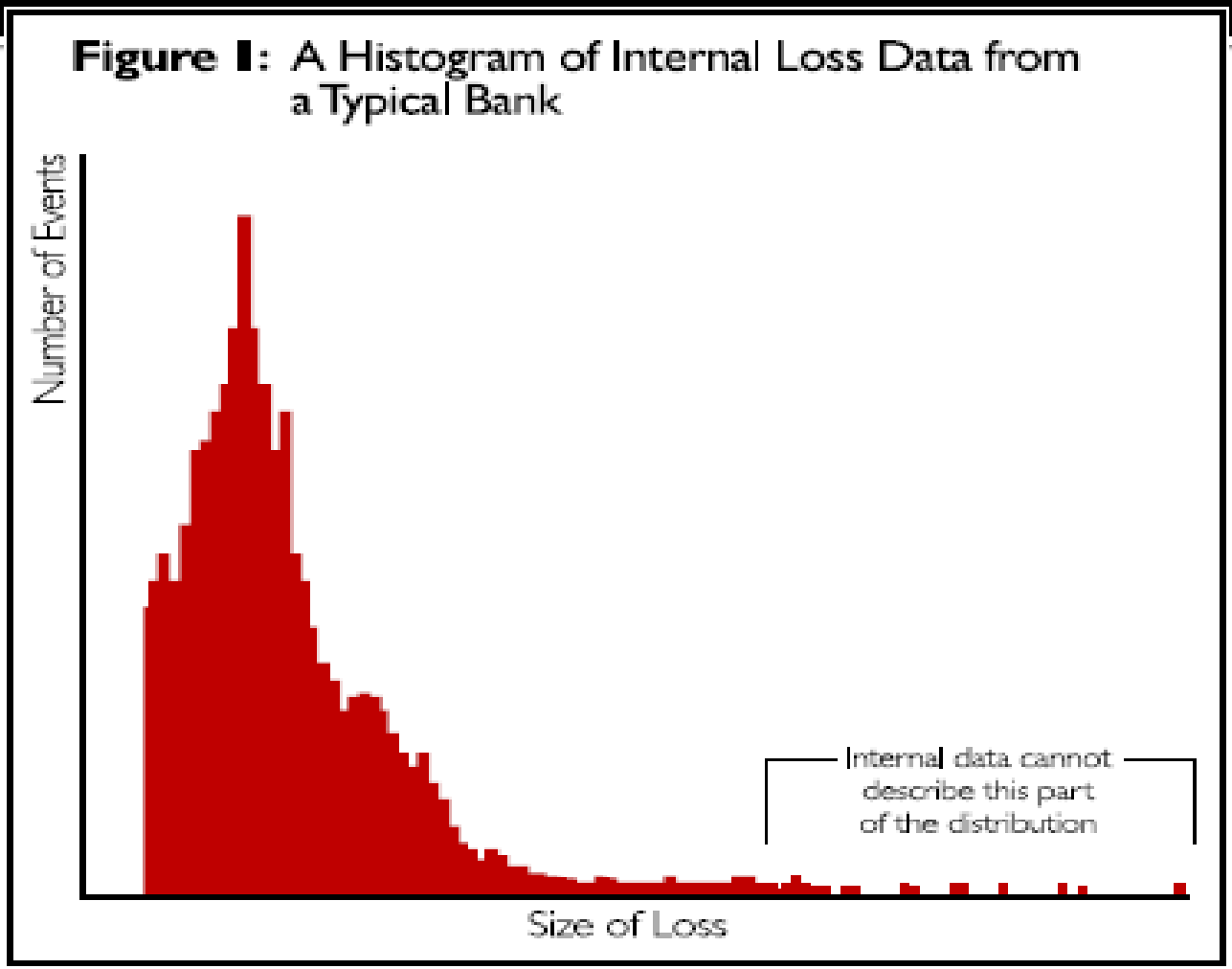
Issues in collection of Loss Data

- **Problems with external loss data - Public**
  - Reporting biases
    - misreporting
    - Non reporting
    - Threshold
    - Lack of necessary details

Issues in collection of Loss Data

- **Problems with external loss data**
  - *Does this mean external data is 'useless'??*
  - No!. Insurance industry has been successfully using external data to calculate expected loss rates and the volatility (confidence intervals) around these estimates.
  - This suggests that there may be scientific ways of addressing these data problems.

Issues in collection of Loss Data



Issues in collection of Loss Data

- **Analysis of a typical set of internal data**
  - If you were to take the internal data from a bank with many years of loss experience and plot it as a histogram, it would probably resemble the graphical illustration in the previous slide.
  - This histogram reveals following facts;
    - that the loss data are collected above a certain threshold
    - that there is a distinct "body" and "tail" to this distribution and
    - that the tail region contains a number of "outliers."

Issues in collection of Loss Data

- **Analysis of a typical set of internal data**
  - The figures actually represents two different risk classes.
    - The body consists mainly of execution errors (primarily high-frequency/ low-severity losses), and
    - the tail consists mainly of losses from other (primarily low-frequency/high-severity) risk classes
    - However, if one were to examine data from the high-severity classes in a large external loss database, one would observe that the data in these data sets are continuously distributed. In other words, these so-called outliers actually do follow a distribution of their own.
    - However, if we were limited to using internal data alone, we would have to wait several thousand years (in a static risk environment) to get to that distribution.

Issues in collection of Loss Data

- **Analysis of external data**
  - There are, broadly speaking, three types of external data — public data, insurance data and consortium data.
  - *Public Data*
    - These data are drawn from publicly available information: newspaper reports, regulatory filings, legal judgments, etc.
    - Contain size based reporting bias.
    - Because of this reporting bias, one cannot extrapolate frequency or severity parameters directly from the data.
  - *Insurance Data*.
    - Insurance data represent losses that have been submitted as claims to insurance companies.
    - These data are captured only in risk classes where the insurance company has offered insurance coverage.
    - Vendor does not reveal the identity of the firms that experienced the losses.

Issues in collection of Loss Data

- **Analysis of external data**
  - *Consortium Data*.
    - These are pooled sets of internal data submitted by member organizations
    - The advantage of consortium over public data is that consortium data are not subject to public (media) reporting biases.
  - Disadvantages are;
    - In some organizations, internal reporting is not yet comprehensive;
    - because consortium data are obtained from many organizations, categorization tends to be less consistent.
    - Consortium data represents only a subset of the loss data universe,

Issues in Collection of Loss Data

- **"Relevance" in the Context of External Data**
  - Making external loss data relevant in connection with the bank's internal loss data, following points need to be considered.
    - *Cautiously consider scaling individual loss data to the size of one's institution*
    - *Be wary of scaling individual losses to the quality of one's internal control environment.*
    - *Don't try and select "relevant" data points from an external database based on the question, "Could this loss happen to me, given my internal control structure?".*
    - *Think carefully before selecting "relevant" data points from an external database based on the question, "Is this organization similar to my organization in terms of control quality?"*

Categorizing Operational Losses

Transaction	Execution	Settlement	Technological
Inadequate Supervision	Information	Key man	Lack of Resources
Reputation	Relationship	Theft	Criminal
Insufficient Training	Unauthorized Activities	Fraud	Rogue Trader
Compliance	Legal	Fiduciary	Physical Assets
Poor Management	Fixed Cost Structures	Customer	Sales Practices
		Business Interruption	People

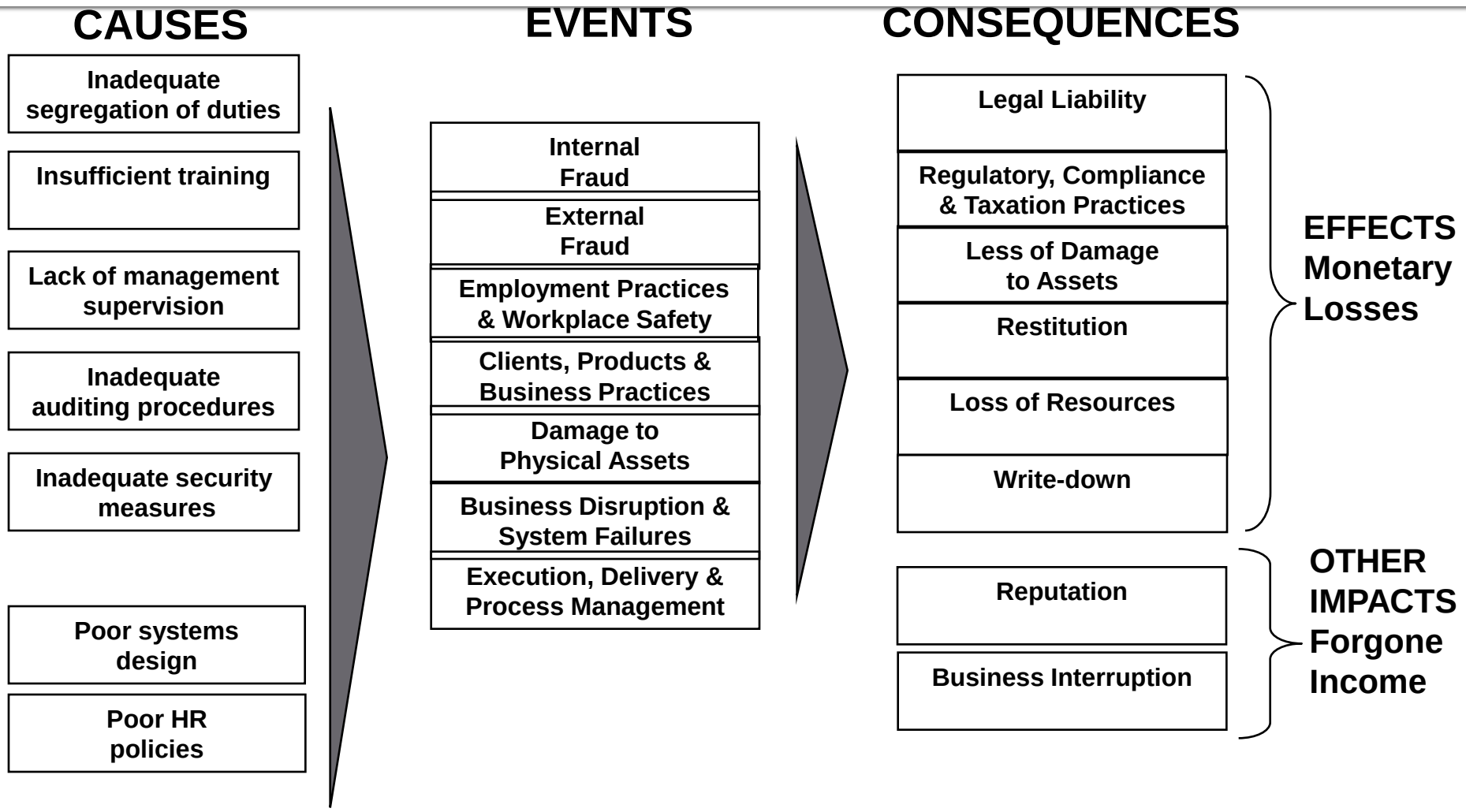
Categorizing Operational Losses

- **'Event' based categorization**
  - BIS framework is designed to be event based approach.
  - There are seven event categories at the primary level.
  - Two of these categories—Clients, Products and Business Practices (CPBP) and Execution, Delivery and Process Management (EDPM)—are defined as mixtures of causes and events,
  - Business Disruption and System Failures (BDSF), another primary category, is defined as a mixture of causes, events and effects
  - Damage to Physical Assets (DPA), primary category, is both an event and an effect.
  - Unauthorized Activities (UA), which is defined as a secondary category under Internal Fraud (IF), actually includes certain non-fraud (negligence-related) events that are very similar to those included in CPBP.

Categorizing Operational Losses

- **The right way to categorize losses**
  - While the risk universe consists of three independent dimensions; causes, events, consequences.
  - It's more logical to look at ops losses in a cause/effect matrix framework.
  - Such an approach helps evolve better, valid and consistent controls

Categorizing Operational Losses



Incident Reporting Format

- Incident reporting is extremely important in order to assess operational risk.
- Without such reporting, it would become very hard to analyze operational losses in the bank for any given time period.
- If incidents are reported truly and regularly, bank management would be able to:
  - Identify areas where losses are occurring frequently.
  - Identify problematic processes.
  - Can take measures to minimize theses losses.

Incident Reporting Format

Head	Descriptions
Date of Loss Event:	Date the incident occurred and date on which reported
Description:	Briefly Explain the Incident
Amount (Before Recovery)	Actual amount of loss
Recovery:	Amount Recovered (Rs.)
Corrective Action	Any corrective action taken to stop similar losses
Reported By:	Name of Reporting Person
Branch/ Group Name:	Name of the Branch and Code / Group

Managing Ops Risk-
The Framework

Managing Ops Risk

An operational risk framework

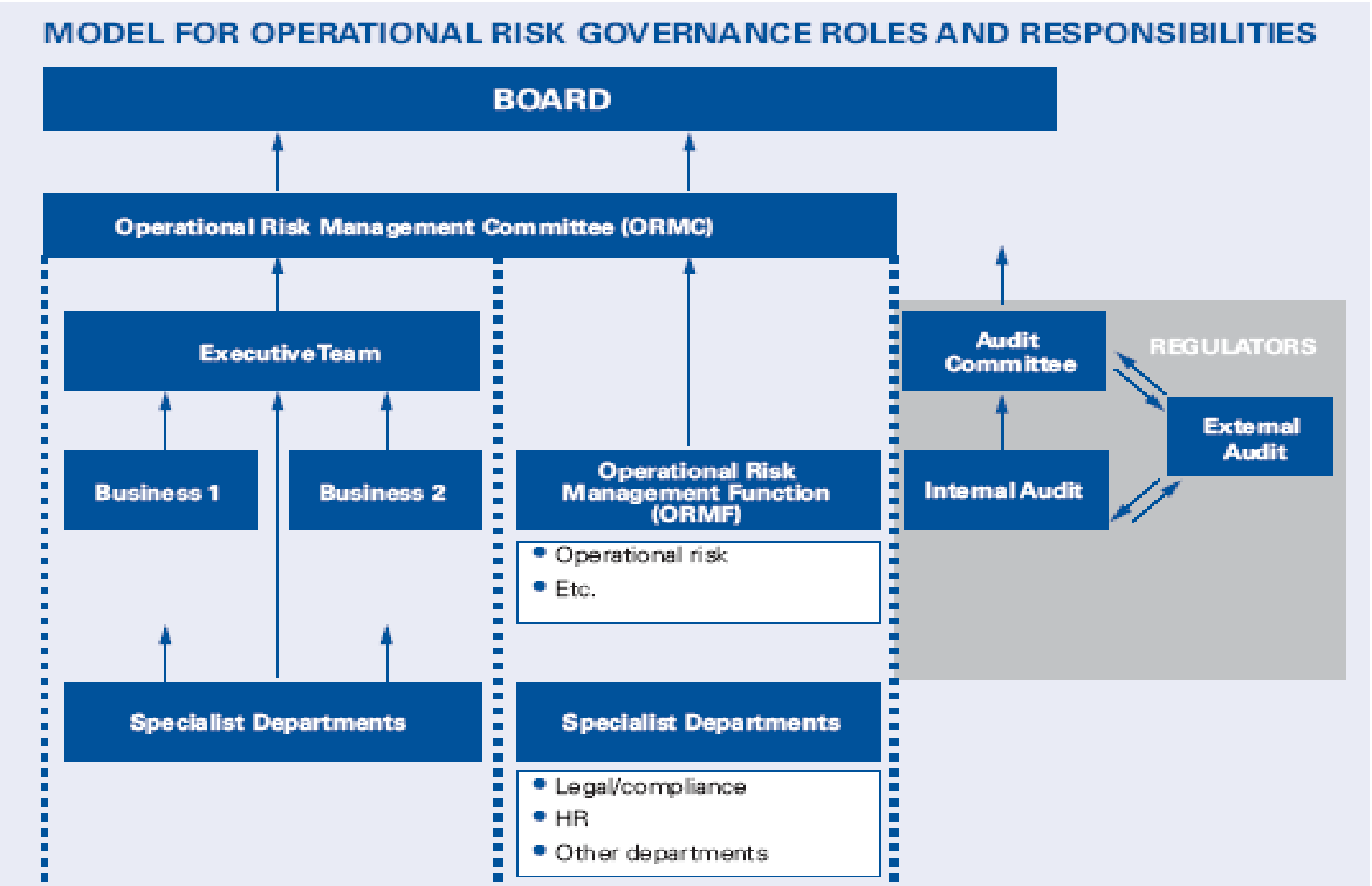
- Operational risk strategy comprises both
  - The "top-down" process of capital allocation and
  - Clear guidance for the "bottom-up" processes of risk identification, assessment, management, reporting and supervision, and governance arrangements that constitute the management framework.
- Setting the risk tolerance/risk appetite
  - Top down – setting thresholds and limits by BoD
  - Bottom up – taking input from RCSA, KRIs, incidents and losses

Managing Ops Risk

Organizational Structure

- Two key goals need to be reflected in an organizational structure for operational risk:
  - The agreement that operational risk cannot be confined to specific organizational units (unlike market risk) but remains largely the responsibility of line managers and some defined special or support functions (such as IT, HR, legal, internal audit, or compliance)
  - The division of duties among management, an (often to be established) independent risk management function, and internal audit.

Managing Ops Risk



ROLES AND RESPONSIBILITIES

PRIMARY RESPONSIBILITY/ DECENTRALIZED	OVERSIGHT/CENTRALIZED	INDEPENDENT ASSURANCE OF ALL OTHER COMPONENTS
• The businesses have primary responsibility for identifying, managing, and reporting their risks. • The businesses are required to manage certain defined risks through the use of facilities and services provided by a specialist risk department (e.g., Corporate Insurance). • Group/Support Functions to report their own risks.	• The ORMF can provide support to the businesses, and review and report key risks to central ORMCs. • The Board and the ORMCs can satisfy themselves that risks are managed cost effectively and to an acceptable level. • Specialist departments can support other parties within the model.	• Internal audit can provide independent assurance of the robustness of the operational risk management processes and methodologies. • Internal audit communicates with external audit and the audit committee.

Reporting

- Oprisk reporting has to cover two distinct aspects:
  - Delivery of defined, relevant operational risk information to management and risk control
  - Reporting of information aggregated by risk category to business line management, the board and the risk committee.

- Whereas the first type of information contains predominantly "raw" data such as losses, near misses, indicators, and risk assessment results, the second reflects aggregated, structured, and often analyzed information designed to provide each level of management with what it needs to enable better operational risk management.

Reporting Framework

Recipient	Type of Information Received
Board	• Aggregated bank-wide information on loss data • Risk assessment and key risk indicators results • Economic and regulatory capital • Ad hoc reports in case of major events
Operational Risk Management Committees	• Aggregated bank-wide information on loss data • Risk assessment and key risk indicators results • Economic and regulatory capital • Ad hoc and detailed reporting of major events

Reporting Framework

Recipient	Type of Information Received
Business-Unit Heads	• Aggregated business unit-specific information on loss data • Risk assessment and key risk indicators results • Economic and regulatory capital • Ad hoc reports in case of major events
Operational Risk Management Function	• Detailed (raw) bank-wide information on loss data • Risk assessments • Key risk indicators

Risk and Control Self Assessment - RCSA

- Risk and control self assessment (RCSA) is a process through which operational risks and the effectiveness of controls are assessed and examined. The objective is to provide reasonable assurance that all business objectives will be met

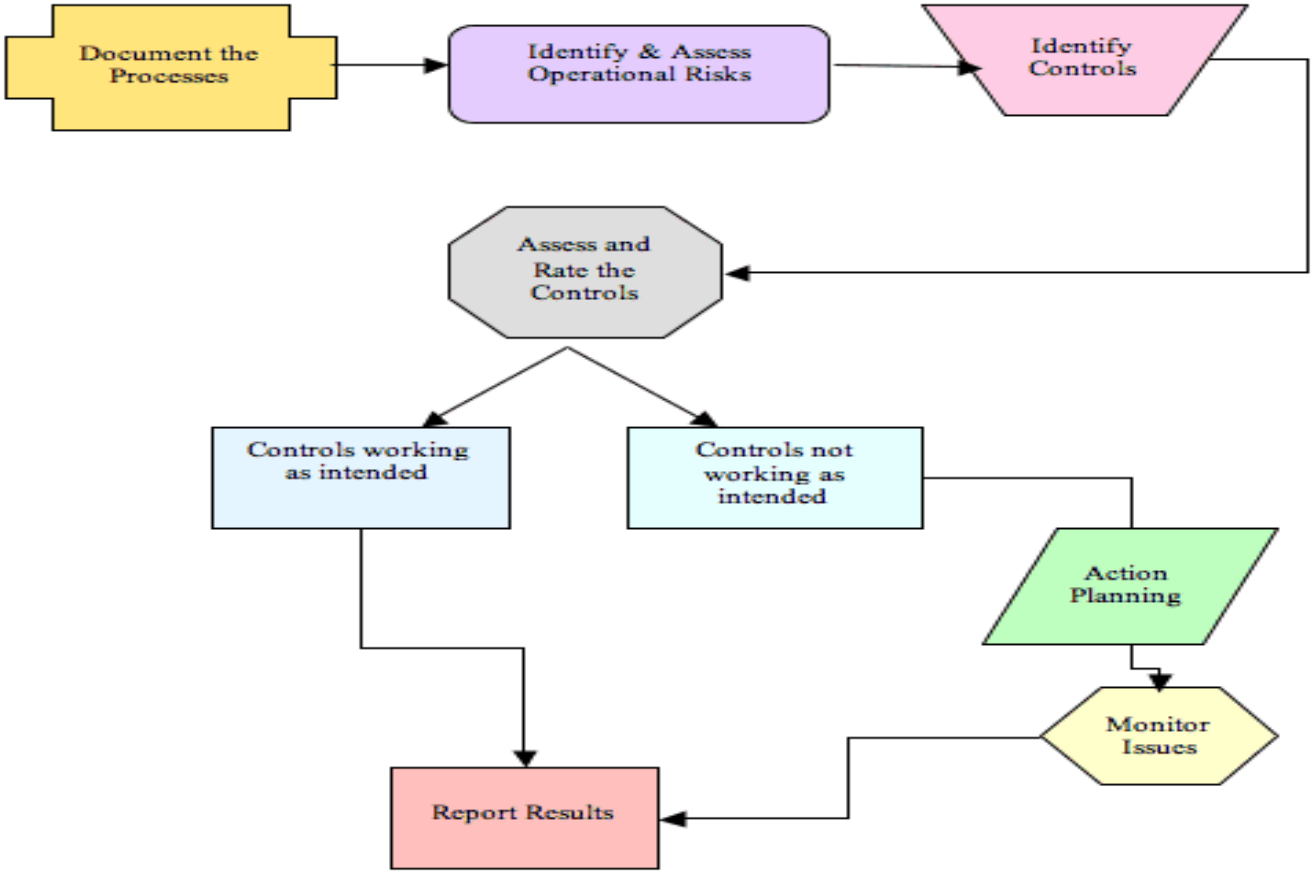
- To establish a consistent, value-added framework for assessing and communicating operational risk and the overall effectiveness of the internal control environment across EGIBL

RCSA - Primary Objectives

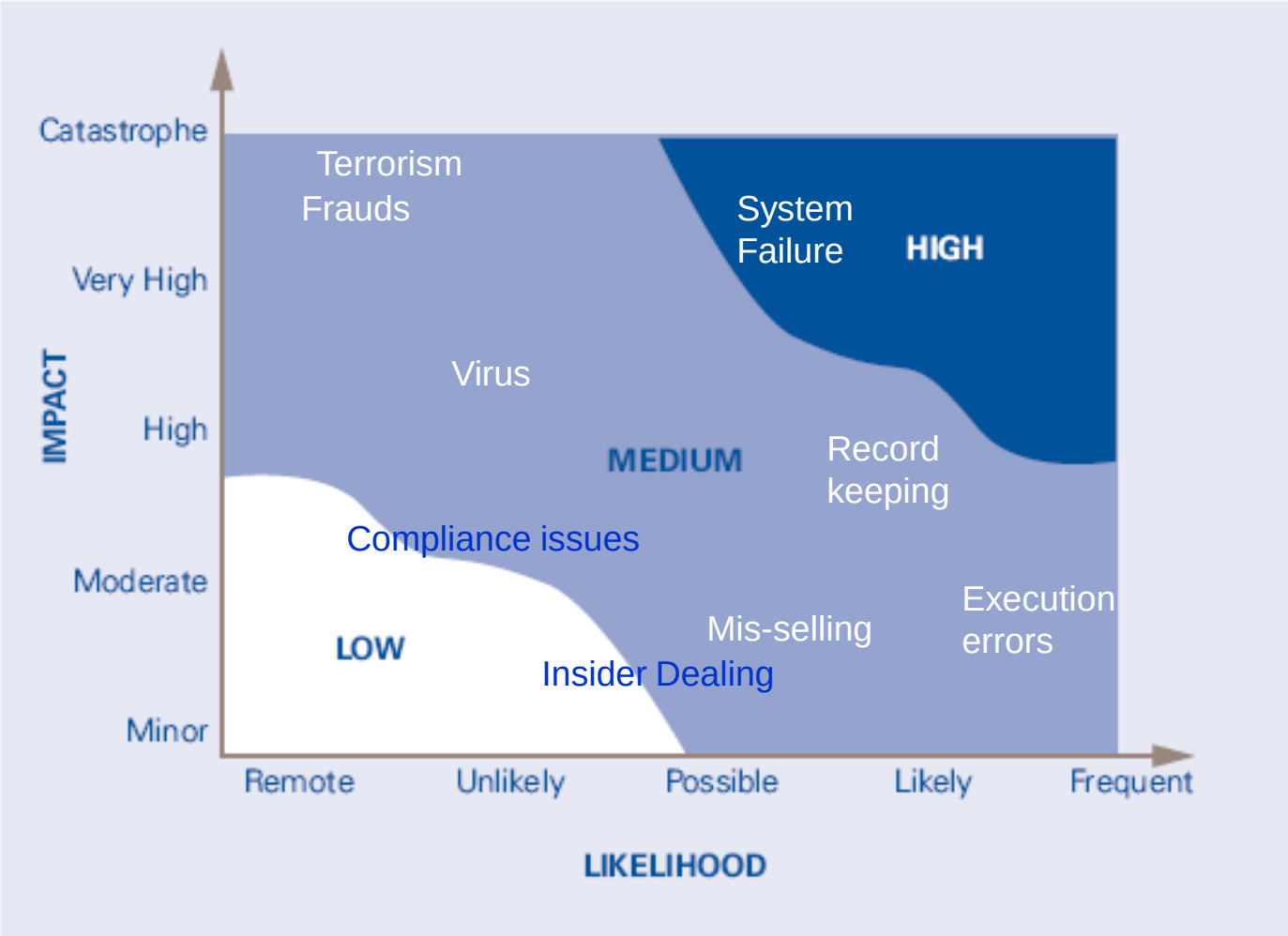
- The reliability and Integrity of Information
- Compliance with policies, plans, procedures, laws and regulations
- The safeguarding of assets.
- The economic and efficient use of resources
- The accomplishment of established objectives and goals for operations or programs

Managing Ops Risk

RCSA – Workflow



Managing Ops Risk



RCSA Benefit

- Encourages both management and staff to assume responsibility for internal controls
- Provides the opportunity to focus efforts on important informal as well as formal controls
- Help organizations to be pro-active
- Reduce audit exposures
- Provides more comprehensive and relevant information
- Looking at the entire spectrum of controls

Managing Ops Risk

Key Risk Indicator: KRI measure level of risk that may affect performance.

- A measure of a specific risk factor
- An early warning signal
- Helps to create "no surprises" culture

Key risk indicators are often insufficiently linked to underlying risk assessment to provide effective risk monitoring

Managing Ops Risk

Types of KRI:

- Leading: Those that measure risk before the event has occurred
- Lagging : Those that measure risk after the event has occurred
- Qualitative: Judgment based
- Quantitative: Lend themselves to more specific actions which can easily measured

Features of a Key Risk Indicator

- Carefully selected and monitored KRI's must be
- forward-looking and help to prevent accidents and losses.
- Behaviors of KRIs should reflect changes in the operational risk profile - (Sound Practices Paper)
- KRIs must periodically be checked for their relevance and accuracy. (Common Sense)
- The search for new KRI's is an ongoing science.

Documenting KRIs

Definition						
KRI Number	0700					
KRI Name	Payments – Number of OFAC Matches Detected					
Description	The number of payment instructions generated during the preceding month where the target country was on the OFAC register of restricted countries.					
Rationale	This indicator measures payments to restricted countries.					
Nature	Current, Lagging					
Type	Exposure Frequency					
Typography	Processes					
Ratings	3	Internal Compatibility	Y	External Compatibility	3	Ease
Specification						
Specification Version	1.0					
Value Format	Count					
Dimensions	1. Location (generating payment) 2. Business Unit 3. Product or Service Group 4. Currency 5. Target Country					
Buckets	1. Indicator values should be divided into time-band buckets reflecting days since payment (medium buckets). 2. Within time-band buckets, the indicator values should be sub-divided into value-based buckets to reflect the number of individual payments of comparable value (medium buckets).					
Bucket Variants	Value buckets may vary for different business lines (for example, investment banking vs. retail banking).					
Currency Conversion	Not applicable					
Measurement Rules	Must include all payment instructions processed during the preceding month where the target country was on the OFAC register of restricted countries.					
Underlying KRIs	None					
Calculation Method	The sum of all items meeting measurement criteria. The indicator value should be calculated for each dimensional node listed above, using the aggregation method and scaling rules stipulated below.					
Benchmark Rules	The indicator value will need to be scaled for benchmarking.					
Aggregation Method	Simple summation using the dimensional nodes listed.					
Aggregation Rules	None specific					
Scaling Denominator	KRI 9749 – Payment Volumes – Total Number of Payments					
Scaling Rules	1. The indicator will be scaled by each 1,000 payments generated. 2. Divide the indicator value by KRI 9749 and multiply by 1,000, rounding the result to 2 decimal places. 3. Aggregate before scaling. 4. Numerator and denominator must be at the same level of aggregation.					
Guidance						
Usage	Internal and Benchmarking					
Collection Frequency	Weekly					
Reporting Frequency	Monthly					
Frequency of Change	Ongoing					
Limitations on Scope	OFAC in US-specific and should be substituted with any other local equivalent in each country where this indicator is used.					
Collection Level	Branch/Operating Entity					
Definition Threshold	Include all payments to OFAC restricted countries, regardless of value.					
Variants	None specific					
Direction Information	Higher indicator value suggests greater risk.					
Trend Information	Increasing indicator values suggests increasing risk.					

Managing Ops Risk

Department	Key risk indicator	Acceptable level	Risk levels		Escalation levels/ Actions/ Responses
Treasury	Fraudulent activities (insider trading, misappropriation of funds, mis-operations etc.) reported	Not acceptable	Low	1 case per yr.	Treasury department will report the matter to the Risk Manager with detailed report.
			Medium	2 cases per yr	RMD will take strict measures to eliminate such a risk by taking strategic decisions which will not hurt the prestige of the company.
			High	3 cases per yr	A complete detailed analysis report will be placed in front of the BRMC with certain suitable recommendations. The board will then analyse the significance of the matter and take strategic decisions.
			Crisis	4 cases and above	Strict measures are taken by the BRMC and penalties are imposed to discourage such actions in future.

Managing Ops Risk

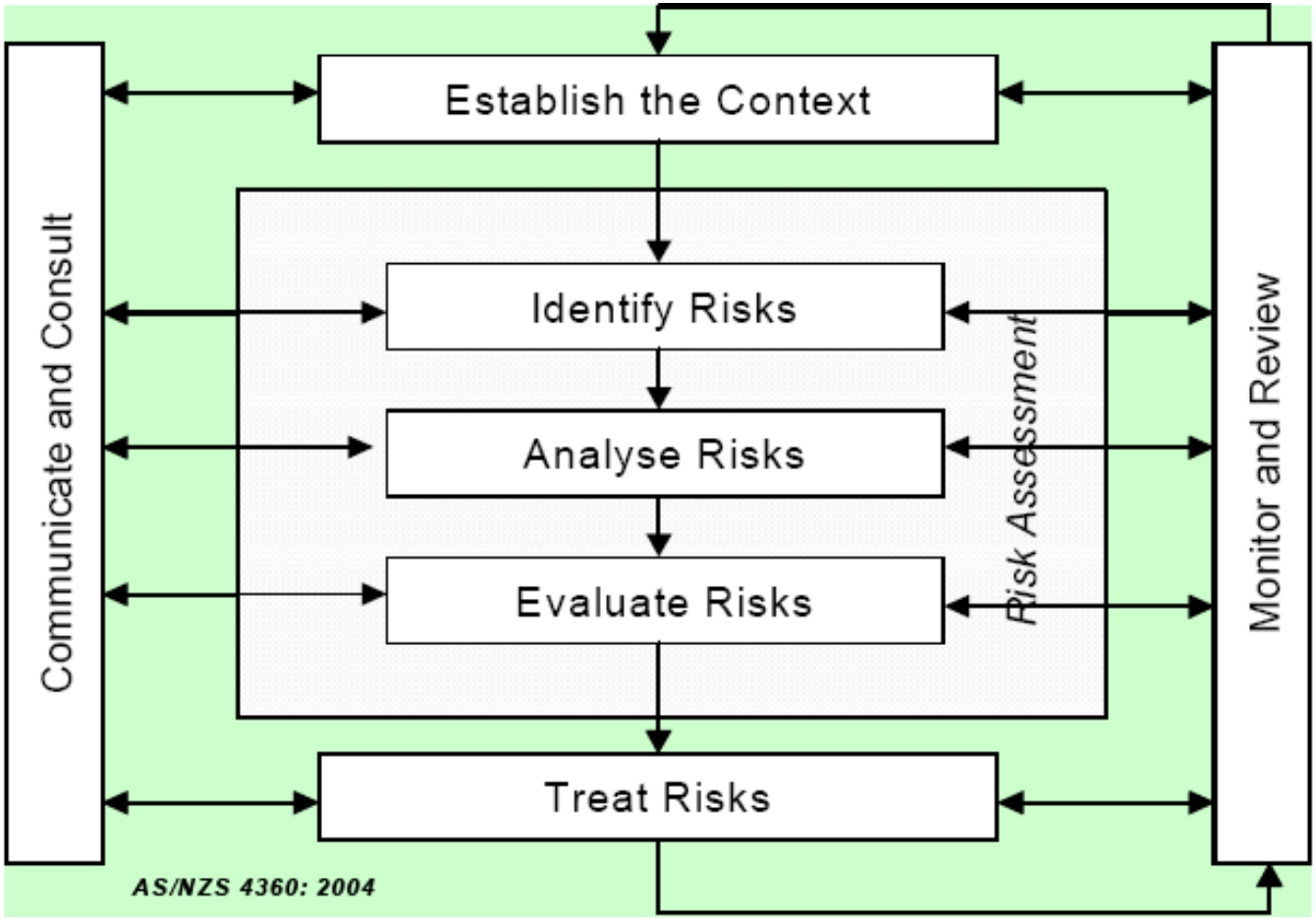
Department	Key risk indicator	Acceptable level	Risk levels		Escalation levels/ Actions/ Responses
Administration	Amount of compensation given to the employee(s) as result of workplace safety event	0.1% of profit after tax	Low	0.1%	Reputation risk will be placed in front of the RMC with detailed analysis of the situation and legal department's recommendations.
			Medium	0.2%	RMC will take all measures to eliminate the risk and report the matter to the BOD.
			High	0.4%	BOD will do complete analysis of the situation and its impact on the company's reputation, cash-flow, employees and clients and will take decisions accordingly.
			Crisis	0.6% and above	Strategic decisions are taken and directions are given by the BOD (i.e., what ever it takes!) to protect the company with reputation risk.

‘Standards’ based approach to Ops risk

'Standards' based approach to Ops risk

- There are mature frameworks from other industries upon which the *processes* of Operational Risk Management could be based
- In particular, there are two risk management standards - AS/NZS 4360/2004 and COSO/ERM – that, alone or in combination, could satisfy the requirements of Basel II for systems that are 'conceptually sound'; and
- The adoption of operational risk management processes that are based on proven, practical and usable standards, should reduce the overall costs to the industry of complying with Basel II.

'Standards' based approach to Ops risk



'Standards' based approach to Ops risk

- **The AS/NZS 4360: 2004 Risk Management Process seven main 'elements':**
  - **Establish the Context**: for strategic, organizational and risk management and the criteria against which business risks will be evaluated.
  - **Identify Risks**: that could "prevent, degrade, delay or enhance" the achievement of an organization's business and strategic objectives.
  - **Analyze Risks**: consider the range of potential consequences and the likelihood that those consequences could occur.
  - **Evaluate Risks**: compare risks against the firm's pre-established criteria and consider the balance between potential benefits and adverse outcomes.

‘Standards’ based approach to Ops risk

- **The AS/NZS 4360: 2004 Risk Management Process seven main ‘elements’:**
  - **Treat Risks**: develop and implement plans for increasing potential benefits and reducing potential costs of those risks identified as requiring to be ‘treated’.
  - **Monitor and Review**: the performance and cost effectiveness of the entire risk management system and the progress of risk treatment plans with a view to continuous improvement through learning from performance failures and deficiencies.
  - **Communicate and Consult**: with internal and external ‘stakeholders’ at each stage of the risk management process.

'Standards' based approach to Ops risk

COSO ERM Framework

Objective: To help business / Financial Institution assess and enhances their Internal Control System.
Framework: Provides BoD and Management a clear roadmap for identifying risk, avoiding pitfall and seizing opportunities to grow stakeholder values

ERM Framework: ERM reflects certain fundamental concepts. Enterprise risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its ris appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

'Standards' based approach to Ops risk

COSO Categories:

This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

- **Strategic** - high-level goals, aligned with and supporting its mission
- **Operation** - effective and efficient use of its resources
- **Reporting** - reliability of reporting
- **Compliance** - compliance with applicable laws and regulations

'Standards' based approach to Ops risk

- **The eight 'components' of the ERM process are (COSO 2004):**
  - **Internal Environment**: establishing the 'tone' of an organization, including "risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate".
  - **Objective Setting**: ensuring that "management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite"
  - **Event Identification**: identifying internal and external events that could impact the achievement of a firm's objectives (both positively and negatively).
  - **Risk Assessment**: analyzing risks "considering likelihood and impact, as a basis for determining how they should be managed."
  - **Risk Response**: selecting 'risk responses' and developing "a set of actions to align risks with the entity's risk tolerances and risk appetite".
  - **Control Activities**: establishing and implementing policies and procedures "to help ensure the risk responses are effectively carried out."
  - **Information and Communication**: identifying, capturing and communicating information that is relevant "in a form and timeframe that enable people to carry out their responsibilities."
  - **Monitoring**: monitor the risk management process itself, modifying it as necessary.

'Standards' based approach to Ops risk

- The COSO ERM Framework

‘Standards’ based approach to Ops risk

Basel II and the standard frameworks

- Basel II identifies the responsibilities of the independent Operational Risk Management function as “developing strategies to identify, assess, monitor and control/ mitigate operational risk”. These responsibilities map directly onto the AS/NZS 4360 and COSO frameworks as shown in the table in the next slide.

'Standards' based approach to Ops risk

- **Basel II and the standard frameworks**

AS/NZS 4360: 2004 Framework	COSO ERM - Integrated Framework	Operational Risk under Basel II
Establish the Context	Internal Environment plus Objective Setting	*Implied by Basel II*
Identify Risks	Event Identification	Identify
Analyse Risks	Risk Assessment	Assess
Evaluate Risks	Risk Assessment	Assess
Treat Risks	Risk Response & Control Activities	Control/Mitigate
Monitor and Review	Monitoring	Monitor
Consult and Communicate	Information & Communication	*Implied by Basel II*

'Standards' based approach to Ops risk

- Combining Basel II with the AS/NZS & COSO

Elements of the AS/NZS & COSO Framework	Primary Responsibilities	ORM Components and Tools
•Establish the Context **•Internal Environment plus Objective Setting**	Board and Senior Management (supported by Strategic Analysts)	- Risk Appetite: Products, Markets and Limits/Tolerances - Risk Regime: Philosophy, Responsibilities, Policies and Procedures - Risk Organization: Oversight, Segregation and Accountabilities - Policies on Ethics, Risk/Reward Incentives and Whistle Blowing - Business and Operational Strategies and Objectives - SWOT Analysis - Communications Plan - Budget Allocations for risk-related Resources and Training

'Standards' based approach to Ops risk

Elements of the AS/NZS&COSO	Primary Responsibilities	ORM Components and Tools
•**Identify Risks** •**Event Identification**	Business Units, (supported by ORM and outside experts)	- Questionnaires, Interviews and Structured Workshops - Control Risk Self Assessment (CRSA) - Brainstorming/Delphi Techniques/Affinity Maps - Process Maps/Flow Charts - Risk Register organized by People, Processes, Systems and External - Expert Judgment - Scenario Analysis
•**Analyze Risks** •**Risk Assessment**	Business Units, ORM and outside experts	- Risk Classification (Likelihood and Impact) - Risk Heat Maps - Loss Events Database - Risk Drivers - Pareto Charts - Failure Mode and Effect Analysis (FMEA) - Cause and Effect (Fishbone) Charts - Sensitivity Analysis - Critical Incidents Analysis - Industry and Organizational Benchmarking

'Standards' based approach to Ops risk

Elements of the 4360 Framework	Primary Responsibilities	ORM Components and Tools
•**Evaluate Risks** •**Risk Assessment**	Business Units, ORM and outside experts	- Risk Assessment, Quantification and Prioritization - Loss Distribution Analysis such as Extreme Value Theory (EVT) - Monte Carlo Simulation - Sensitivity Analysis - Bayesian Belief Networks - Causal Modeling - Calculation and Allocation of Capital Charges - Identification of Key Risk Indicators (KRIs) - Stress Testing
•**Treat Risks** •**Risk Response**	Business Units, ORM and outside experts	- Risk Treatment Options (Avoid, Reduce, Share, or Retain/Accept[18]) - Cost/Benefit Analysis of Risk Treatments - Risk Treatment Planning, Resourcing and Cost/Benefit Tracking - Risk Treatment Communications Plan - Business Continuity Planning

'Standards' based approach to Ops risk

- Advantages of adopting a Standards Based Framework
  - Cost Savings
  - Risk Reduction
  - Training and Education
  - Resources
  - Independent Expertise
  - IT Systems
  - Outsourcing

Basel II - Challenges & pitfalls

- **Challenges**
  - Organizational Sponsorship
  - Business Line Buy-in and Resources
  - Coordination with Existing Control Initiatives
  - Development of Loss Databases
  - Well-Designed Methodologies and Models
  - Access to Appropriate Information and Reporting

- Mistaking Operational Risk for Market or Credit Risk

Basel II - Challenges & pitfalls

- **Pitfalls**
  - Waiting for the regulators to provide detailed guidance and lay out an implementation road map
  - Failing to make the link between information, technology, risk management and the business
  - Attempting to build a Basel II infrastructure without data and technical architecture road maps
  - Underestimating the magnitude of cultural change that Basel II requires

THANKS!