Operational Risk Management:

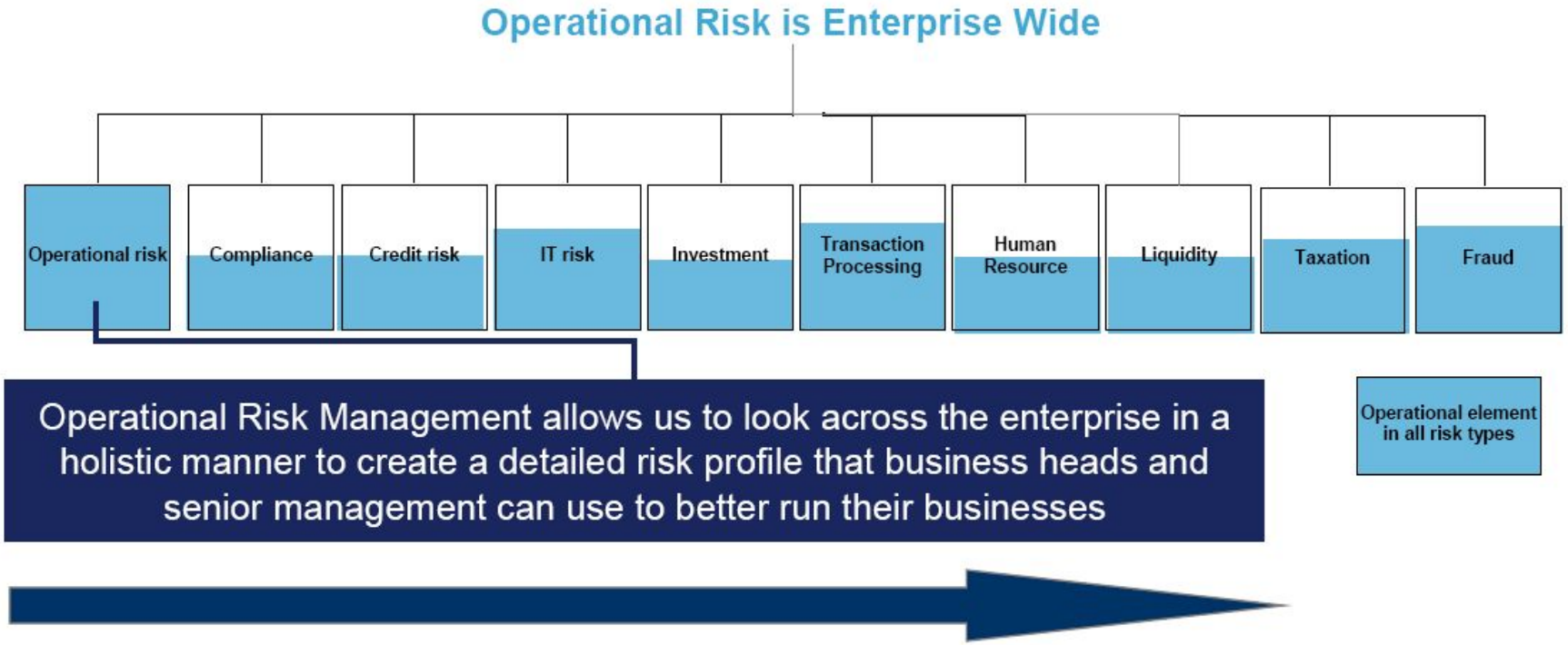
Best Practice Overview and Implementation

Table of Contents

Table of Contents

Table of Contents

OpRisk IS AN ENTERPRISE-WIDE RISK



OR has been managed already before it has been „labelled— so. However ORM has **never been an integrated process**, rather a set of fragmented activities to deal with a wide variety of risks

RECENT OUTSTANDING OPERATIONAL LOSSES

BARINGS PLC – 1995, USD 1.3 Bln – unauthorized trading by Nick Leighson.

Mizuho Securities – Dec 2005 (USD 250 Mio) – trader error (sold 620 K shares for 1 yen, instead of 1 share for Yen 620K) – shares sold over 4 times the outstanding shares in the company; failures at Mizuho, incl. —fat finger‖ syndrome, and TSE clearing failures.

SG – Jan-2008 Euro 4.9 bio net (or 6.3 bio gross of unauthorized profile of Euro 1.4 bio) – unauthorized

- trades, false hedges, risk measured on net basis,
- password management, knowledge of controls, weak
- controls; —culture of tolerance‖, ignoring warning
- signs, incentive structure of traders….etc.

UBS – credit write-downs related to sub-prime exposure of over $ 38 bio. S&P downgraded rating one notch to AA- and may lower further due to —risk management lapses‖. Tier 1 ratio would fall to 7% without capital increase and rights issue (an ELEMENT OF OPERATIONAL RISK within this credit risk loss).

US Mortgage Crisis – non-registration of mortgage loans – instead of registering security interest with local authority, banks did it with a parallel MERS (owned by them) – 64 Mio mortgages under question.

Major Losses Raise Importance of Incident Management

International Soft Regulation of Operational Risk

ISO Standards:

31100 – Enterprise Risk Management;

27900 – Information Security

FERMA (Federation of European Risk Management Associations)

Standards

IOR Guidance

2009 - OpRisk Appetite;

03/2010 – Risk Control Self Assessment; 09/2010 – Governance

11/2010 – KRI;

09/2011 – Risk Categorization;

11/2011 – External Loss Events

EBA (CEBS) Guidelines

06/2010 – Market Activities OR;

09/2011 – Internal Governance;

01/2012 – AMA Extensions & Changes

BCBS

02/2005 – Outsourcing;

06/2006 – Basel 2;

08/2006 – Business continuity;

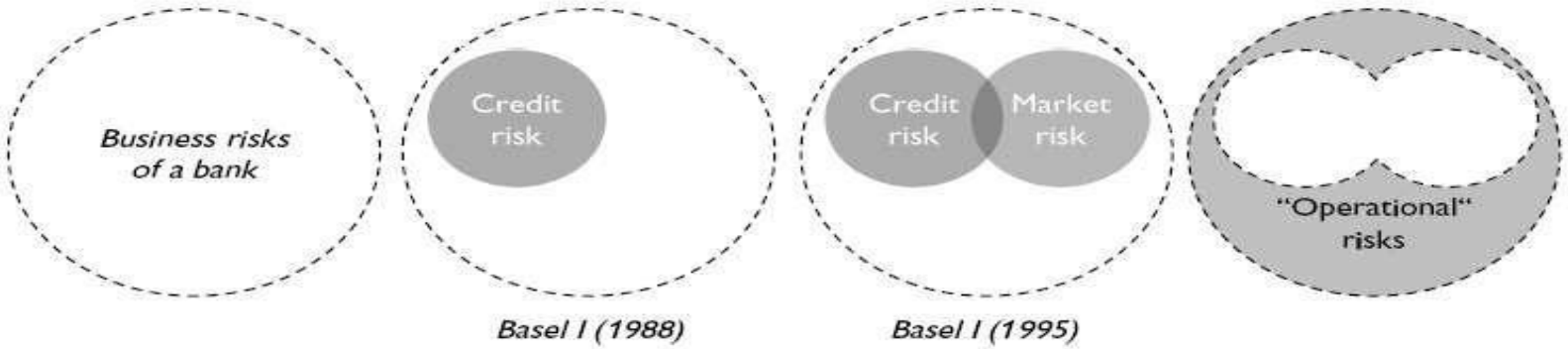
11/2007 – Home-Host Supervision;

10/2010 – Insurances for AMA;

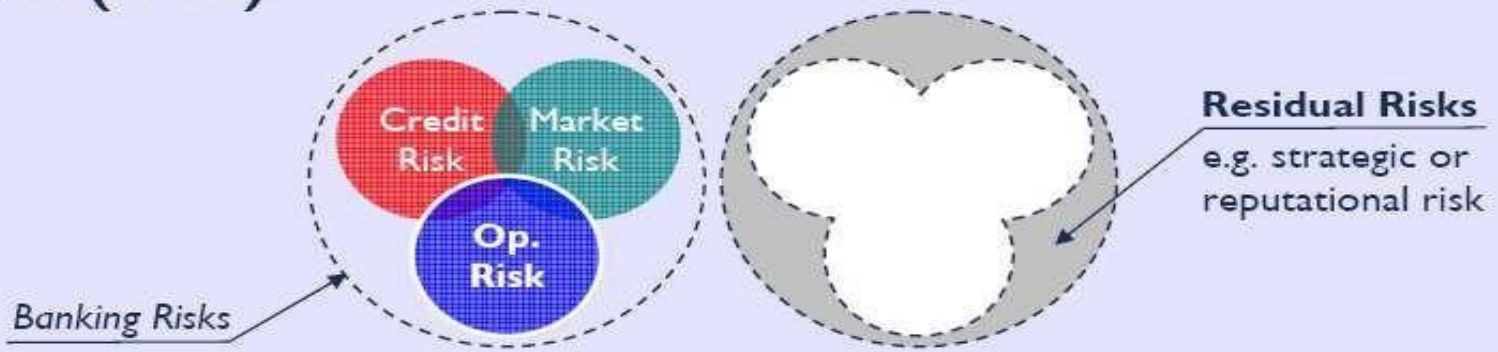
11/2010 – Guidelines AMA;

06/2011 – Principles of OpRisk Sound

INTERNATIONAL REGULATORY PERCEPTION OF the companyING OR



- **Basel II (2004)**



Supervisors „discovered— OR as separate risk class => Don_t get trapped into finding a perfect definition

DEFINE OpRisk PRIOR TO MEASURING IT

„Narrow“
(Basel 2, §644, R.Morris Ass.)

Risk of losses resulting from:

(1) **inadequate or failed internal processes,**

(2) **people and**

(3) **systems or**

(4) **from external events**

including legal risk (as fraud constitutes the most significant OR loss events category and a legal issue**,**

excluding strategic & reputational risks

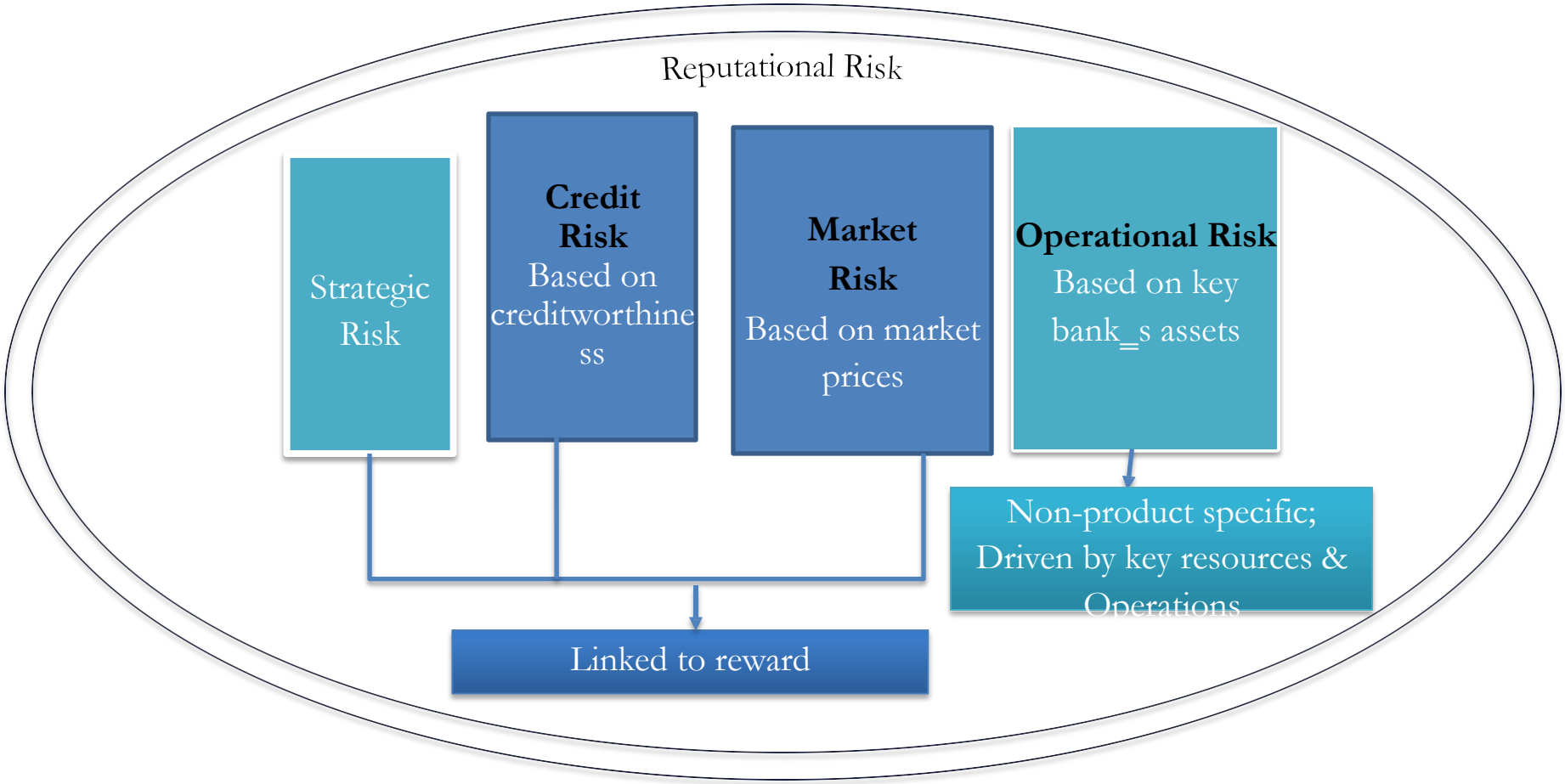
„Wide“

BCBS definition is *artificial,* for regulatory capital calculation.

- The largest OR component - Business risk - OMITTED
- Reputational risk (biggest biz risk!) EXCLUDED

—All risks, other than credit and market, which could cause volatility of revenues, expenses and value of the company‘s business.‖

BANKING RISKS



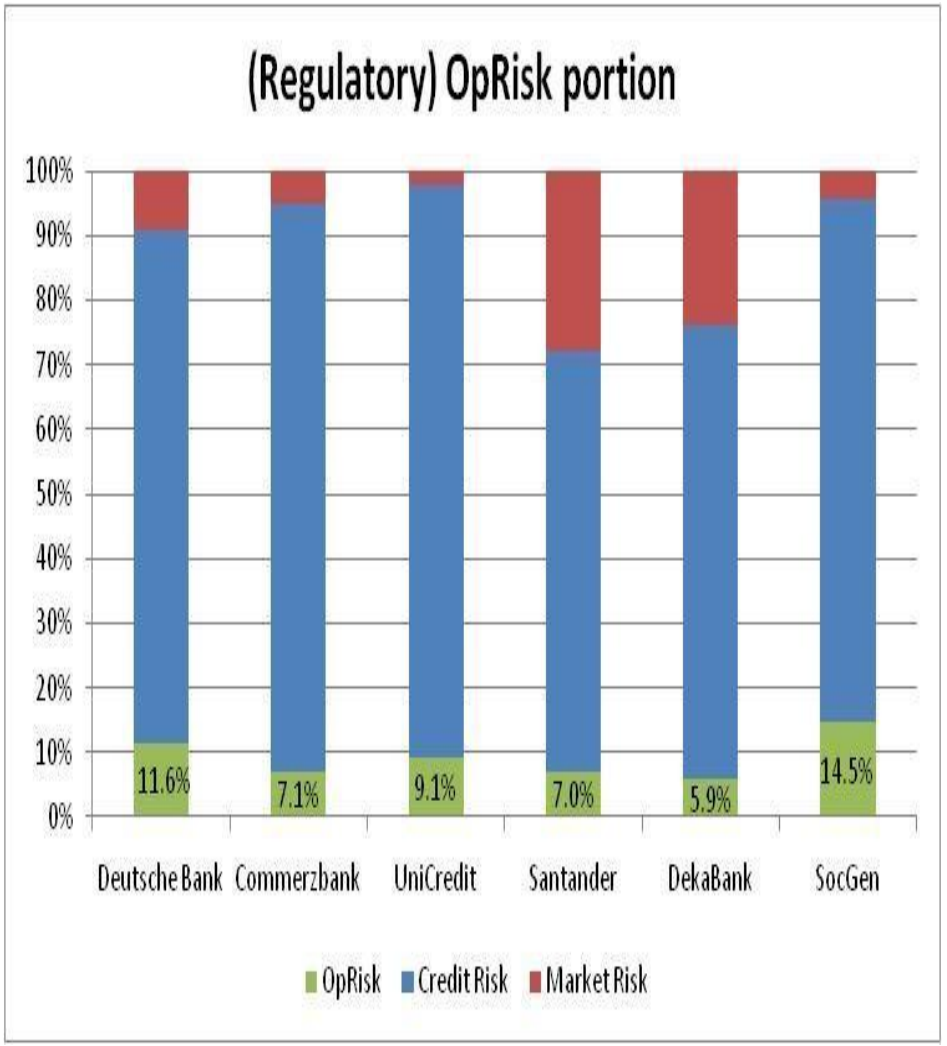
Credit and Markets Risks are specific to the financial industry **vs**
OpRisk - a general business risk with particular features in banking. OpRisk is taken not because of financial reward (like credit & market risks), but exists in a normal course of business activity;

OPERATIONAL RISK PORTION IN REGCAP

OpRisk

- **Diverse in its scope**
- Encompasses the risks emanating from **all** areas of business
- **Complex** in causes, sources and manifestations
- **One-sided**, no risk/return trade-off inherent to market and credit risks
- **No** well established **quantitative** approaches
- **Fewer** resources dedicated
- **Multiple skills required** (know-how, self learning capacity, etc.)

- **Banks' key resources = main risk drivers for op risk!**
- OpRisk: ~ 10 percent of total regulatory capital

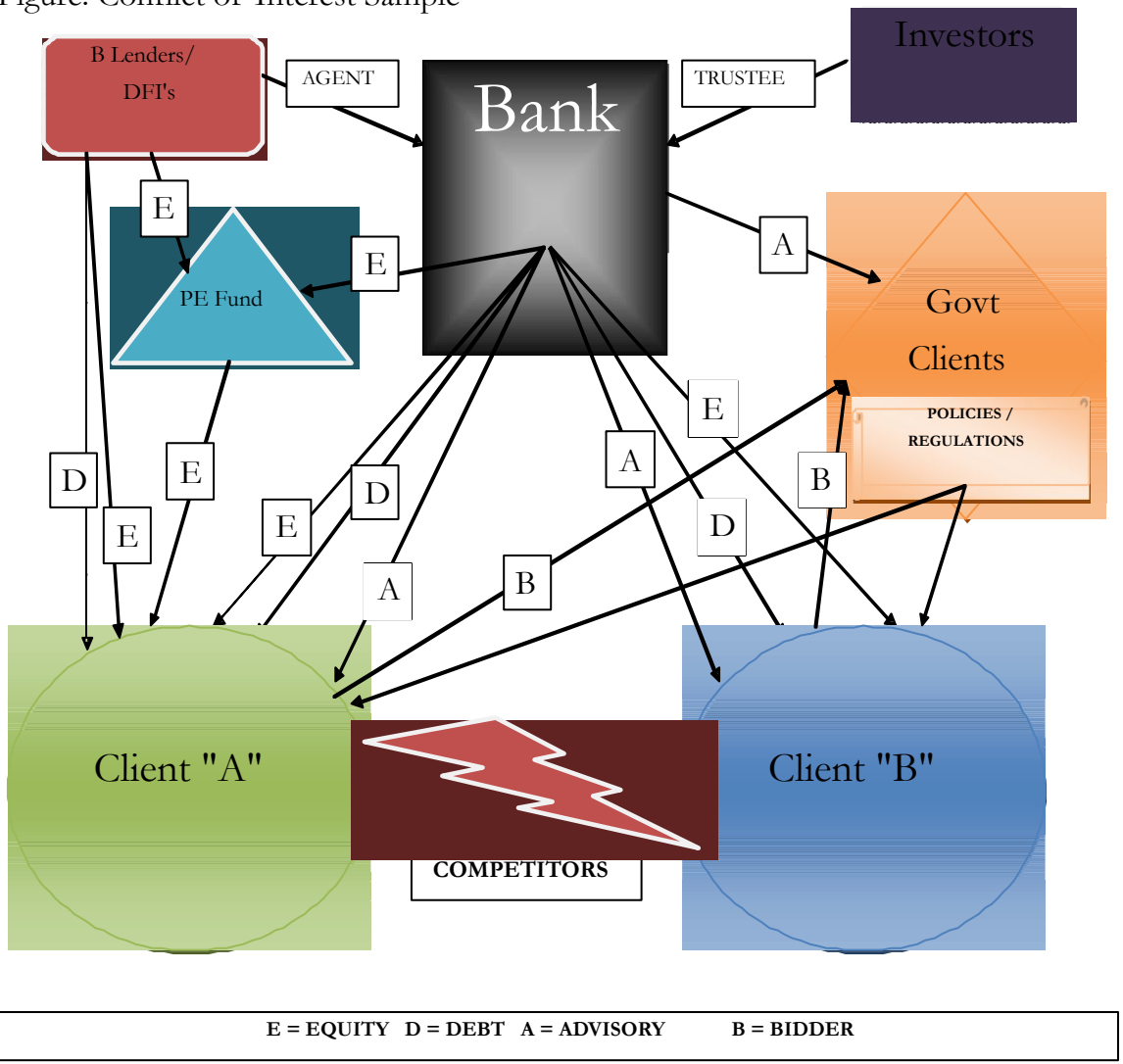


MANAGEMENT RISK - #1 OpRisk

Management Risk components:

- conflicts of interest
- excessive pay levels
- breach of fiduciary duty
- mismanagement
- unjust enrichment
- waste of corporate resources;
- 45% of finance top-managers prepared to commit economic crimes

Figure: Conflict of Interest Sample



LEGAL RISK

Causes of legal risk materializing

- Breakdown of the law enforcement —industry‖
- Corruption
- Political & Occult interests
- Exploitation of loopholes in the law

- *Financial products are not protected neither with copyright, nor licensing!* –
- Business may be lost to non-banking institutions

Legal risk components

- Legal proceedings (lawsuits) adversely affecting bank's financial position, results of operation, liquidity, resulting from:

-contracts;

-Torts;

-Derivative actions

- Documentation risk – linked to information risk;
- [Regulatory] Compliance – civil, administrative & criminal liability of the company and/or its officers
- [Cross-border] insolvency proceedings

REPUT RISK INCLUSION INTO THE ORM

- **Reputation** is a key asset of a fin institution, as it represents the its past and future prospects, describes its attractiveness for the stakeholders, as compared to competitors.
- **Risk Quantification is** difficult *(IRM runs RepTrak Pulse)*.

- **3 elements** of RepRisk mngt:

(1) Crisis mngt (acute risks mngt) – based on catastrophic OpRisk mngt

(2) Risk mngt (latent reputational challenges)

(3) CSR

- Main RepRisk mngt measure – efficient interaction with stakeholders, as their human perceptions rule the fin institution‘s reputation. Important to define the real key stakeholders.

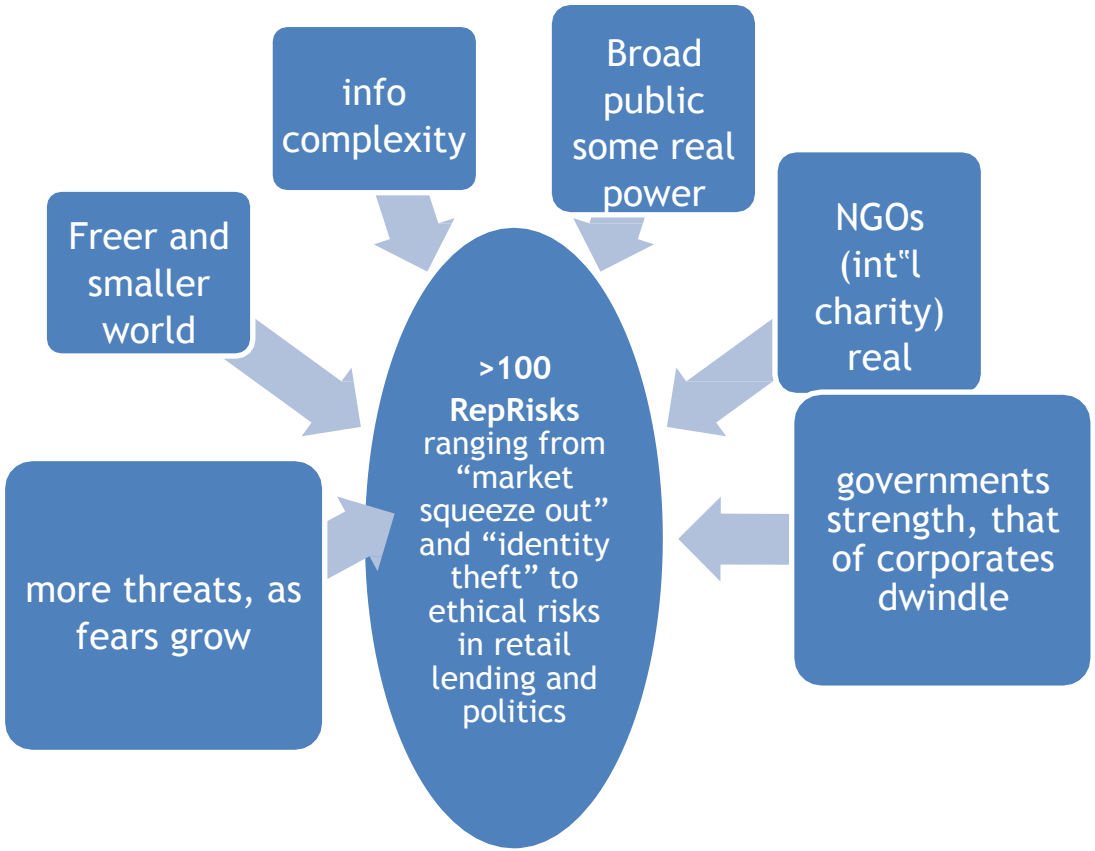
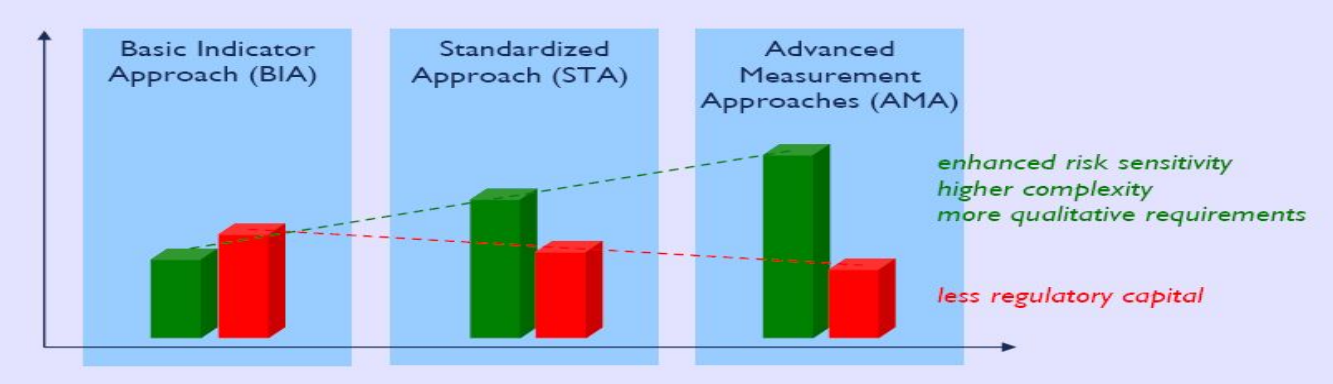


Table of Contents

BASEL-2 PILLARS ON OpRisk

Pillar 1 Minimum Capital Requirements (Objective: limit risk taking)	Pillar 2 Capital Adequacy (Objective: Improvement of banks internal risk management)	Pillar 3 Disclosure (as risk taking & management tool)
OpRisk Capital Approaches: 1. Basic Indicator (BIA, compulsory) 2. Standardized (TSA, ASA, optional) 3. Advanced Measurement (AMA, optional)	Issues addressed under the supervisory review process … **C. Operational risk** 778. Gross income, used in the Basic Indicator and Standardised Approaches for operational risk, is only a proxy for the scale of operational risk exposure of a bank and can in some cases (e.g. for banks with low margins or profitability) underestimate the need for capital for operational risk. With reference to the Committee document on *Sound Practices for the Management and Supervision of Operational Risk* (February 2003), the supervisor should consider whether the capital requirement generated by the Pillar 1 calculation gives a consistent picture of the individual bank's operational risk exposure, for example in comparison with other banks of similar size and with similar operations. Reference to „Sound Practices for Management & Supervision of OR—	Capital Requirements for op risk Risk exposure and assessment Operational risk Disclosure ❑Quantitative ❑ Qualitative -Definition -Strategy -Governance -Risk Quantification (explanation of Data Aggregation mechanism…) -Risk management (limits, planning, etc.) …

B2/PILLAR 1: ORM QUANTITATIVE & QUALITATIVE REQUIREMENTS



OpRisk Capital allocation: 15% of average 3-y gross income

Rec: implement sound practices paper

Fixed % of G-income by 8 bizlines

- BOD & Sr.Mngt involvement;

-Responsibilities for OR function& policies;

-OR loss collection;

-OR Monitoring;

-BizLine Mapping

Measured by Bank's Internal Systems

- BOD & Sr.Mngt involvement;

- Independent OR Function

-Systematic OR reporting integrated into mngt;

OR losses collection (3-5 yrs);

Scenario assessment

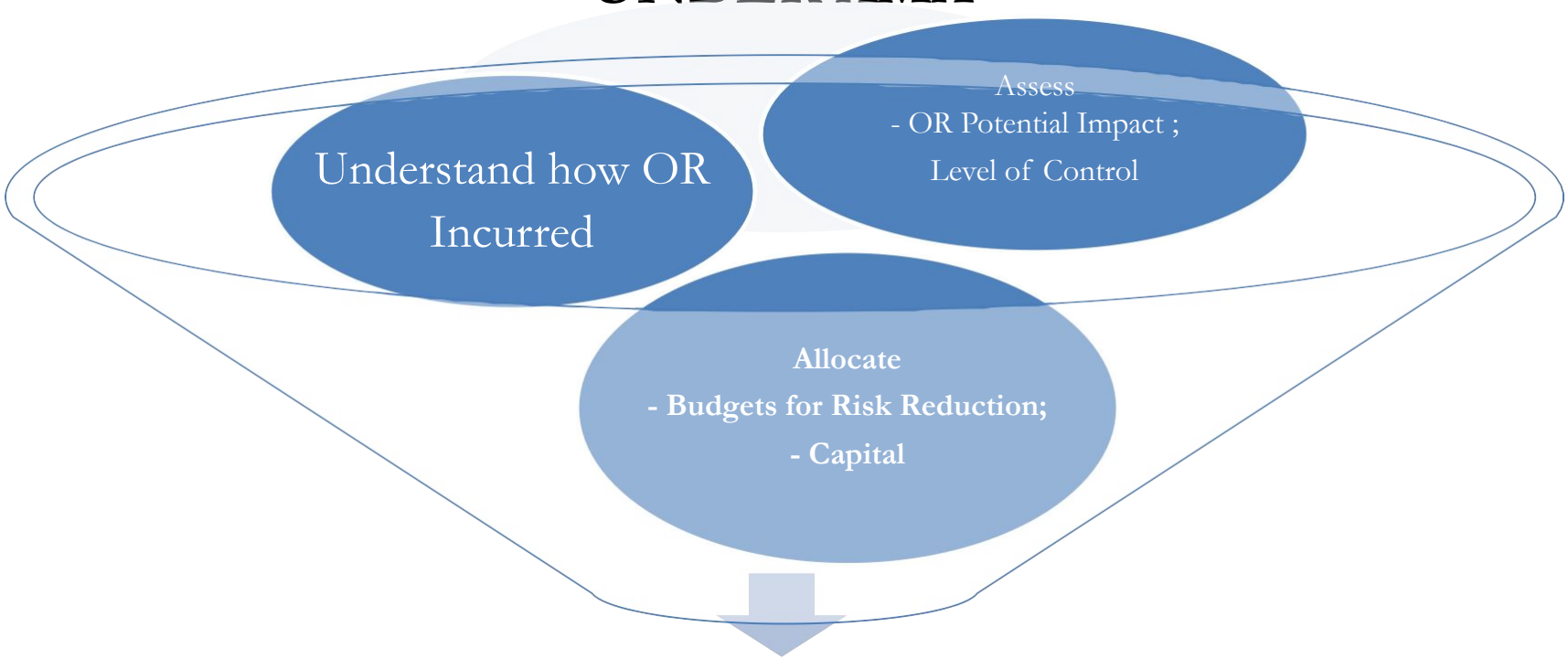
Regular Independent Review by internal & external auditors;

Recognition of insurance

Business environment & internal control

STAGES OF ORM DEVELOPMENT IN A BANK

GOALS OF OPERATIONAL RISK MANAGEMENT UNDER AMA

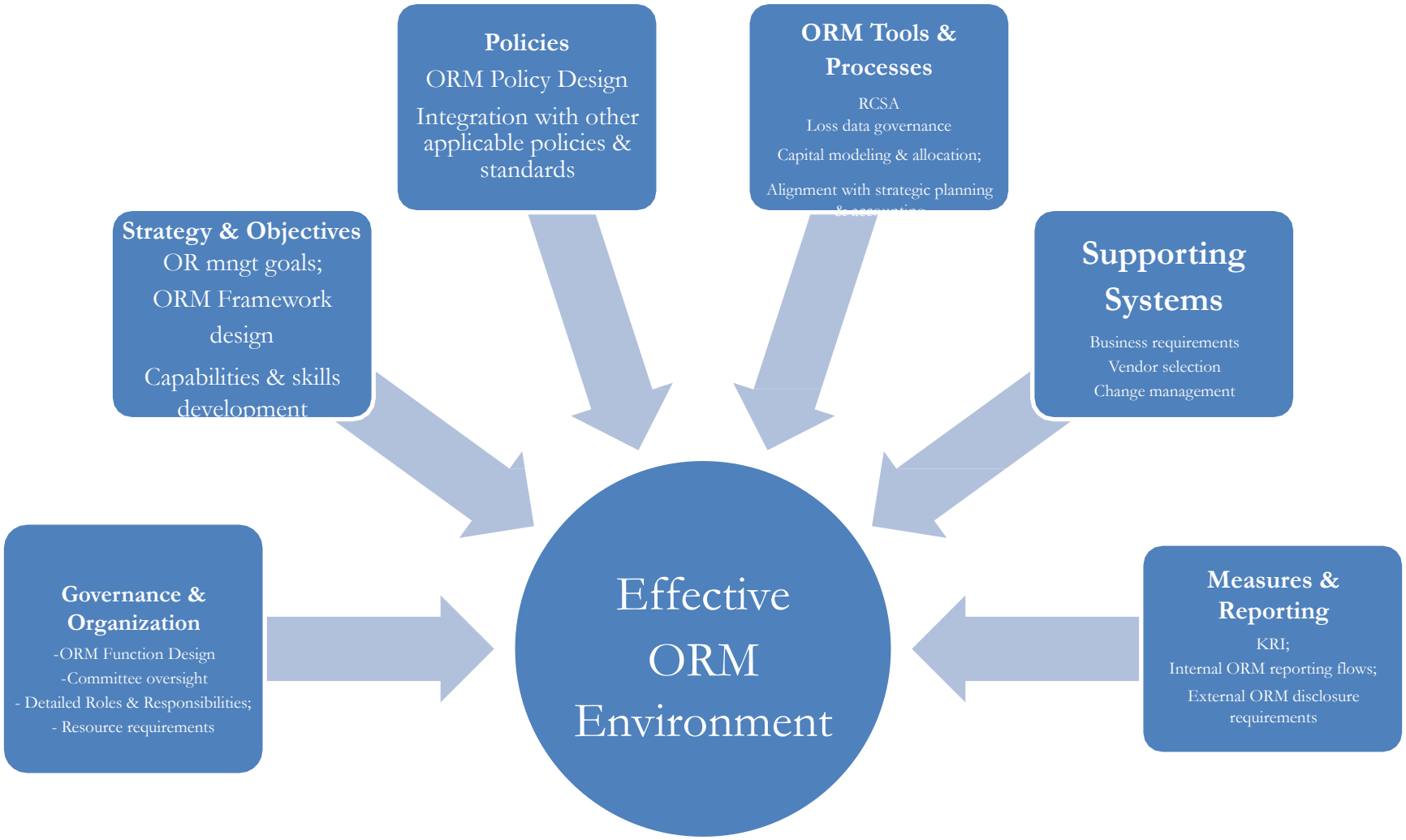


Increase results

Reduce Risks

Improve Product Quality

COMPLEX BASEL AMA RISK GOVERNANCE FRAMEWORK



B2/PILLAR 2: PRINCIPLES FOR THE SOUND MANAGEMENT OF OpRisk (JUNE 2011)

OpRisk mngt is e*specially important* for material & new products, activities, processes & systems.

Monitor & report material ops risk profiles & losses.

Effective control & mitigation change Risk Profile &/or Appetite

Fundamental Principles (PP 1-2)

Risk Management Environment (PP 6-10)

Risk Governance (PP 3-5)

Role of Disclosure (P11)

FUNDAMENTAL PRINCIPLE 1: BOD's Leadership

… and ultimate responsibility for strong **ORM culture**

Internal **OR culture** = a combined set of individual and corporate values, attitudes, competencies and behavior that determine a firm's commitment to and style of ORM.

BOD shall establish a code of conduct, identify acceptable business practices and prohibited conflicts.

Compensation policies shall be aligned to the company's **risk appetite**, appropriately balancing risk and reward

BOD shall ensure the OR training available at all levels throughout the organization.

RISK CULTURE

Includes:

(1) Integrity and ethical values;
(2) Management philosophy & operating style;
(3) Organizational structure;
(4) Delegation of authority & responsibility;
(5) HR policies and practices;
(6) Staff competencies.

Driven by:

- BOD & sr mngt commitment
- HR practices

-OR training and awareness campaigns;

-Working environment;

- Communication style (internal as well as disclosure to stakeholders of ORM practices and position)

Risk mgnt indicators	Lead to	Contribute to
Risk events reporting	Lessons learned	Risk Optimization thru staff behavior
drives		
Risk mngt info	Opportunities to intervene	
influences		
Risk mngt process	Actions to mitigate risk	
creates		
Risks values and rewards s-m	Staff motivation	

OP RISK APPETITE (ORA)

"the amount and type of risk an organization is prepared to seek, accept or tolerate" (ISO 31100). Cost / benefit decision needed to define. OR more complex than CR and MaRisk, simple limits won't suffice.

Setting ORA

ORA must be owned by the MB and established with its engagement.

Top-down cascade from the MB – bizlines add detail, increase level of granularity

Qualitative expression = risk culture = series of absolute statements in the biz strategy

Quantitative expression based on hard info, combining KPIs, KRIs, KCIs. Might bear zero-tolerance, compare to peer group.

ORA is based on agreed thresholds, that shall be sufficiently sensitive to provide early warning of potential ORA breaches, not hypersensitive to ring needlessly.

Use **RAG** (Red-Amber-Green) scale to assign status.

Applying ORA

1. Monitoring to early warn
   - **Reporting** INTEGRAL (*complete, accurate, timely*) data by an appropriate party at an agreed frequency;
   - **Converting** data to information by adding context and interpretation.
2. Aggregation and reporting.
3. Decision making, as a choice between
   - Accepting the breach
   - Mitigating the breach & avoiding its recurrence
   - Intermediate management action (intense monitoring, root cause analysis, investigating the cist/benefit of mitigating action.

Escalation policy for events over a threshold or KRI needed

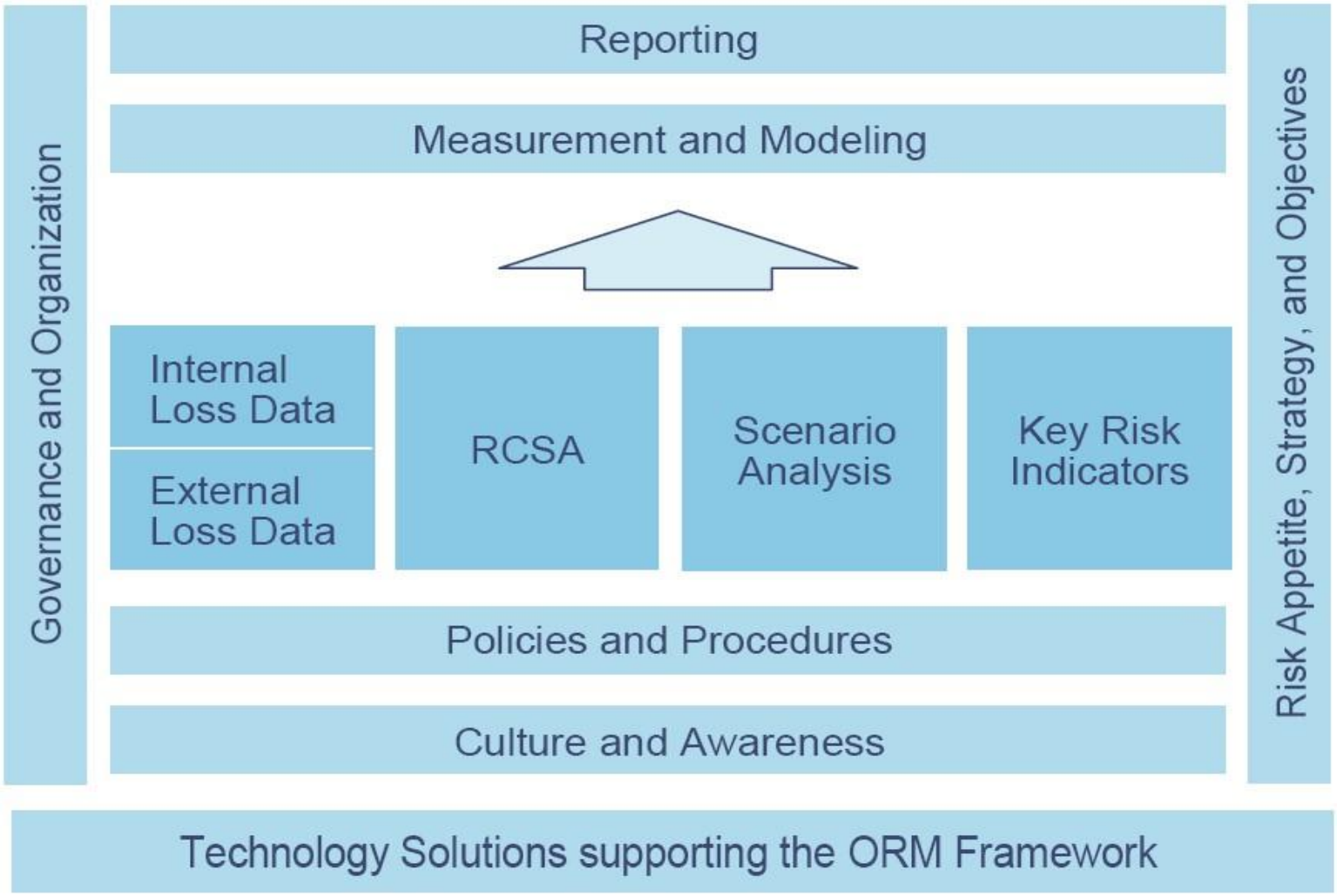
Fundamental P2: OpRisk framework integrated into overall risk management processes

It depends on size, complexity and risk profile of bank.

Framework documentation shall:

- Identify the governance structures, theirreporting linesand accountabilities;
- Describe risk assessment tools and their usage;
- set methodology for establishing and monitoring thresholds, or limits for inherent and residual risk exposure;
- Establish risk reporting and management information systems;
- Provide for a common taxonomy of OR terms to ensure consistency of risk identification, exposure rating and mngt objectives

B2: AMA – EXAMPLE OF ORM FRAMEWORK



MANAGING OpRisk THROUGH FRAMEWORK

OR has been managed already before it has been „labelled— so:

- „4-eyes—-principle,
- separation of functions,
- allocation of responsibilities and limits,
- internal controls and their review by auditors.

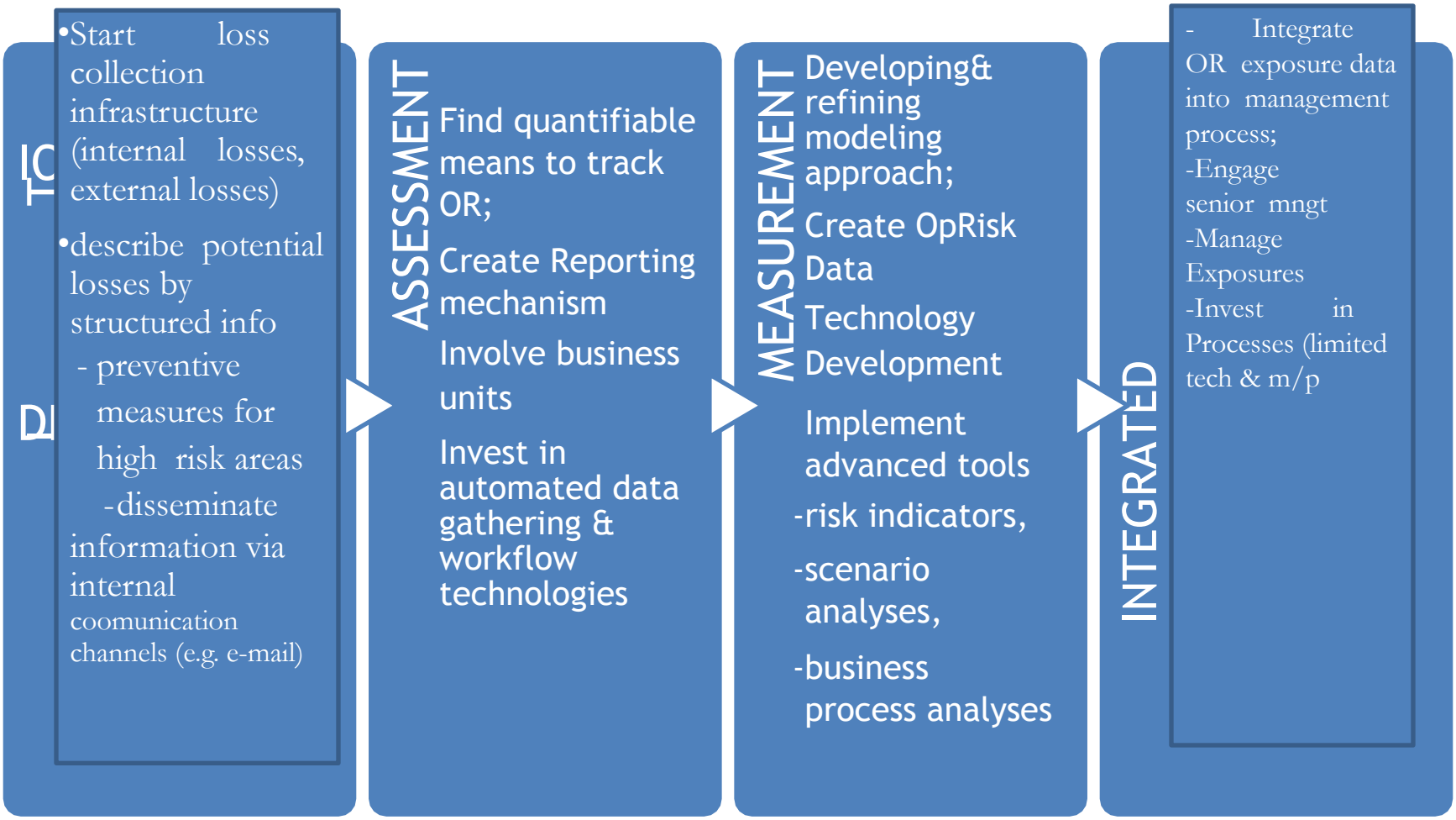
ORM has **never been an integrated process**, rather a set of fragmented activities to deal with a wide variety of risks

ORM shall be a tenacious process, not a program

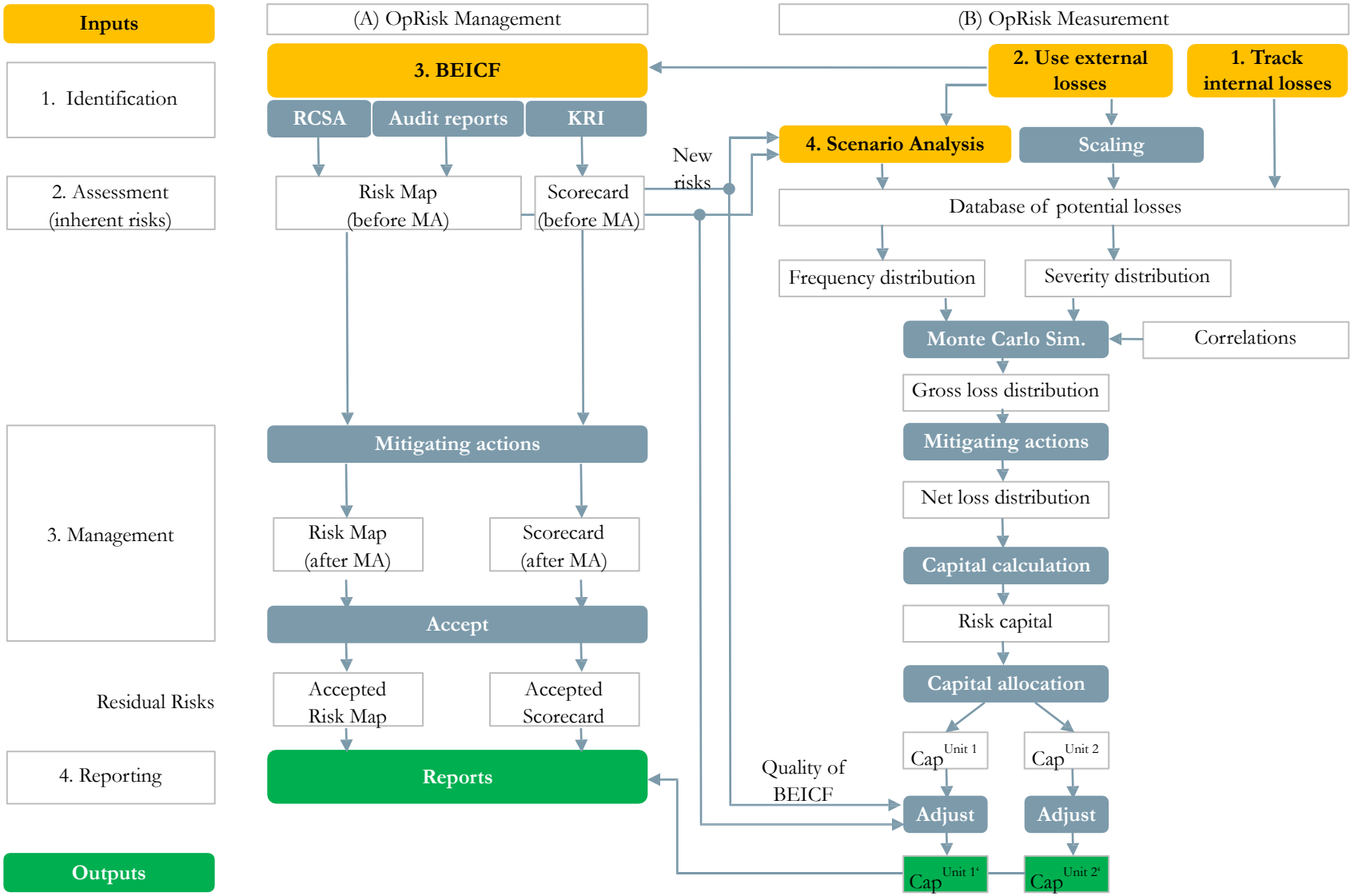
- Prevention ahead of correction
- Ongoing questioning of 6Ss- —Strategy-Structure-Systems-Safety-Simplicity-Speed‖
- Risk awareness with everyone;
- Further the risk culture rather then controlling numbers
- ORM for own sake ahead of its management for supervisors

OR now managed via a —framework‖ since touches all aspects of bank

ORM FRAMEWORK IMPLEMENTATION



EXAMPLE OF COMPLEX ORM FRAMEWORK



P6. Operational Risk Assessment

Assessment of operational risk in all material products, processes and systems. Identification considers external and internal factors.

Tools include:

audit findings,

internal loss data collection and analysis,
external data collection and analysis,

risk assessment,

biz process mapping,
risk and performance indicators,

scenario analysis,

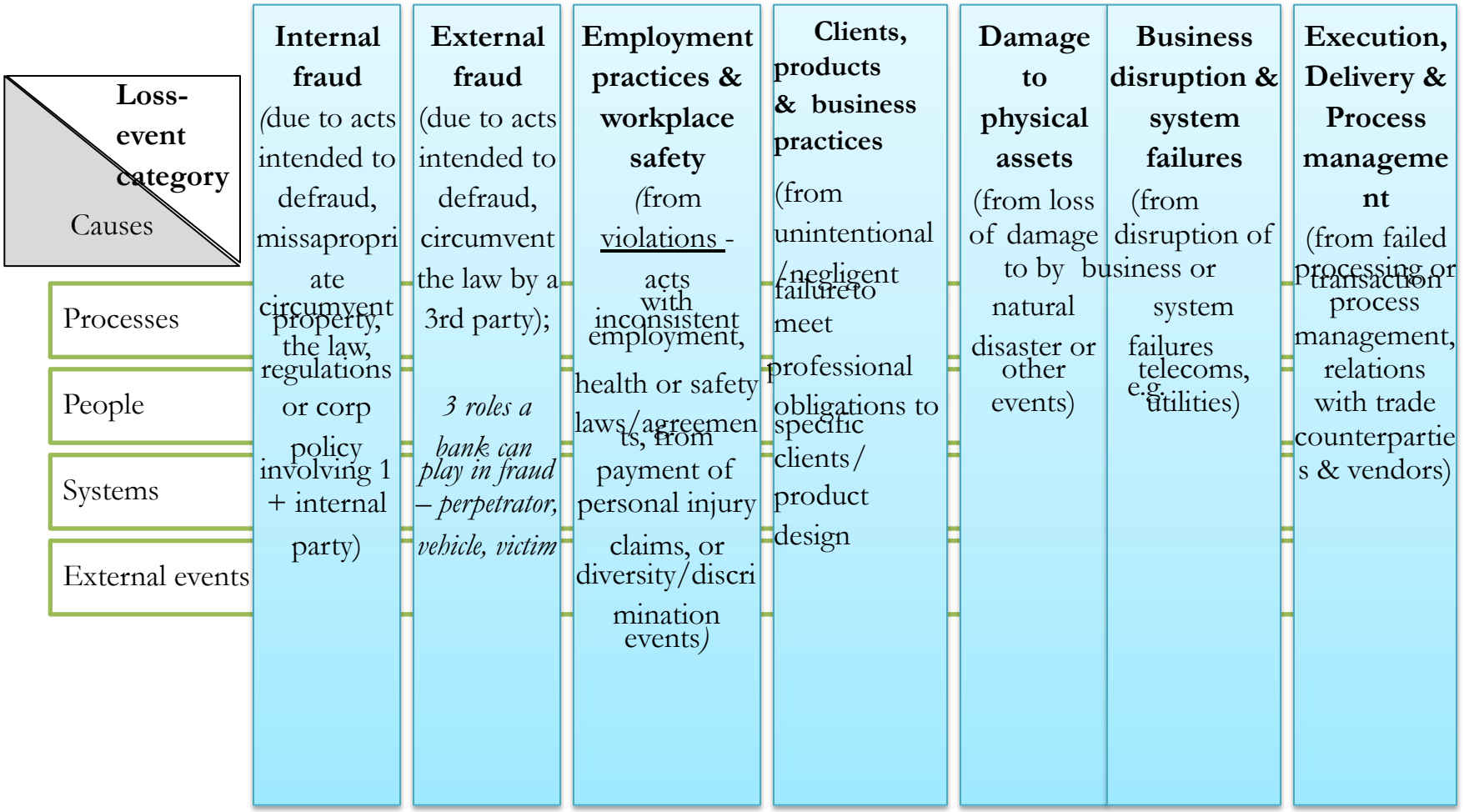
measurement,

comparative analysis (e.g. frequency and severity data with results of RCSA).

LOSS TYPES

Loss type	Causes	Monetary loss
Legal and liability	Lost legal suit	External legal and other related costs in response to an operational risk event.
Regulatory, compliance and taxation penalties	Penalties paid to the regulator	Fines or the direct cost of any other penalties, such as associated costs of license revocations – excludes lost/ foregone revenues
Loss or damage to assets	Neglect, accident, fire, earthquake	Reduction in the value of the firm‘s non-financial assets and property
Restitution	Interest claims Note: excludes legal damages which are addressed under legal and liability costs	Payments to third parties of principal and/ or interest, or the cost of any other form of compensation paid to clients and/ or third parties
Loss of recourse	Inability to enforce a legal claim on a third party for the recovery of assets due to an operational error	Payments made to incorrect parties and not recovered. Includes losses arising from incomplete registration of collateral and inability to enforce position using ultra vires.
Write downs	Fraud, misrepresented market and/ or credit risk	Direct reduction in value of financial assets as a result of operational events.

BASEL 2, 2D-CLASSIFICATION – EVENT/CAUSE BASED



OP LOSSES: CAUSE CATEGORIES & ACTIVITY EXAMPLES (1-3, 5)

Internal Fraud

- **Unauthorized Activity** (transactions intentionally not reported; transaction type unauthorized w/o monetary loss), intentional mismarking of position
- **Theft and Fraud** (Credit Fraud/ worthless deposits; Extortion / robbery / embezzlement; misappropriation / malicious destruction of assets; forgery, check kiting, account take-over; tax non-compliance/evasion; bribes/kickbacks$ insider trading (not on firm's account)

External Fraud

- **Theft & Fraud** (Theft, Robbery, Forgery, Check kiting)
- **Systems Security** (Hacking Damage, theft of information w/o monetary loss)

Employment Practices & Workplace Safety

- Employee Relations (Compensation, benefit, termination issues; organized labor activity);
- Safe Environment (general liability; employee health & safety rules events);
- Diversity & Discrimination (all discrimination types)

Damage to physical assets

- Disasters and other events (natural disaster losses; human losses from external sources – terrorism, vandalism)

OP LOSSES: CAUSE CATEGORIES & ACTIVITY EXAMPLES

Clients, Products & Biz Practices

- **Suitability, Disclosure & Fiduciary** (fiduciary breaches / guideline violations; Suitability / disclosure (KYC, KYCC); Retail customer disclosure violations, breach of privacy, aggressive sales; account churning, misuse of confidential information;
- **Improper Business / Market Practices** (Antitrust; Improper Trade/Market practices;
- **Product Flaws** (product defects; model errors);
- **Selection, Sponsorship & Exposure** ((Failure to investigate client; Exceeding client exposure limits);
- Advisory Activities (disputes over their performance)

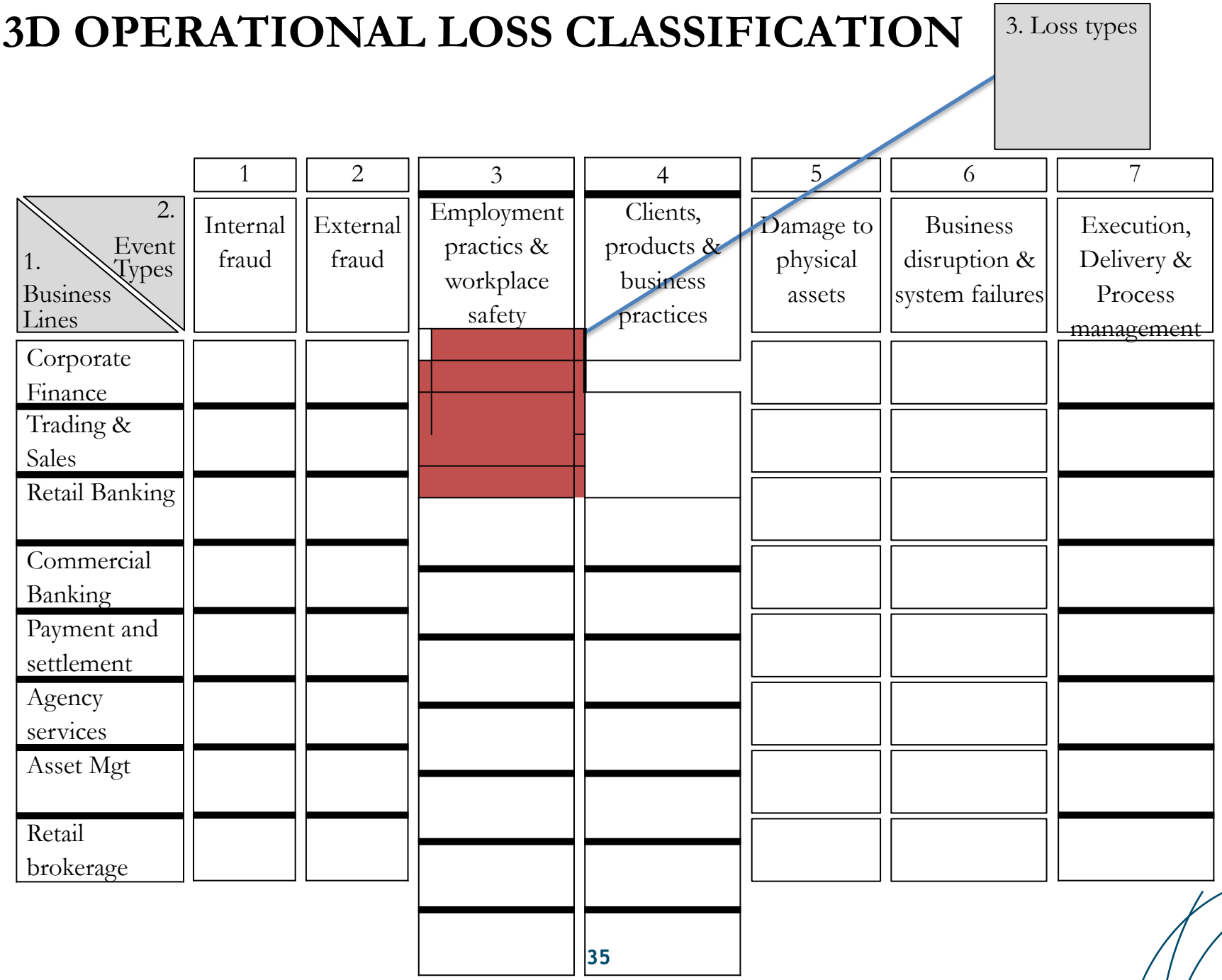
Biz Disruption & System Failures

- Hardware;
- Software
- Telecommunications;
- Utility outage / disruptions

Execution, Delivery & Process Mngt

- Transaction Capture, Execution & Maintenance (Miscommunication, Data entry / maintenance / loading error; Misused deadline / responsibility; model/system mis-operation; Accounting / entity attribution error; other task mis-performance; delivery failure; collateral management failure; reference data maintenance);
- Monitoring & Reporting (failed mandatory reporting obligation; inaccurate external report)
- Customer Intake & Documentation (client permissions/disclaimers missing; legal documentation missing/incomplete);
- Client Account Management (unapproved access provided to accounts; incorrect client records (loss incurred); negligent loss or damage of client assets)
- Trade Counterparties (non-client counterparty mis-performance; non-client counterparty disputes)
- Vendors & Suppliers (Outsourcing; Vendor Disputes)

3D OPERATIONAL LOSS CLASSIFICATION



RISK MANAGEMENT ENVIRONMENT

-OpRisk shall be managed as a distinct category of risks

-Set principles for OpRisk mngt

-Subject ORM framework to audit

-Sr mngt responsible to implement an ORM framework

P7: Senior mgt ensures existence of approval process for all NEW products, activities, processes and systems. Review and approval process should consider inherent risks, changes in the risk profile, necessary controls, risk mngt processes & mitigation strategies, the residual risk, the procedure and metrics to measure monitor and manage the risk of new products. **Special attention** to M&A that can undermine bank's ability to aggregate and analyze info across risk dimensions.

P8: Senior mgt ensures regular monitoring by appropriate **reporting mechanisms.** Reports shall:

(1) Be manageable in scope and volume,

(2) Be Timely

(3) Include breaches of the thresholds/limits, details of significant internal OR loss events, relevant external events

P10: Bank should have business resiliency and continuity plans.

RISK MANAGEMENT CONTROL ENVIRONMENT (P9)

I. Internal controls:

1) clearly established authorities for approval;
2) monitoring of adherence to assigned risk thresholds / limits,
3) safeguards to access to bank assets and records;
4) HR: appropriate staffing + a 2-weeks vacation policy;
5) regular reconciliation of accounts;
6) process automation coupled with sound techno governance and infrastructure RM programs;

II. Risk mitigation strategies

1) top-level progress reviews,
2) review of treatment and resolution of instances of non-compliance,
3) tracking reports and approved exceptions.

NB! Assignment of conflicting duties without dual controls / other countermeasures may enable concealment of losses, errors, etc. Areas of potential conflicts of interest should be identified minimized and subjected to monitoring and review.

III. Risk transfer strategies

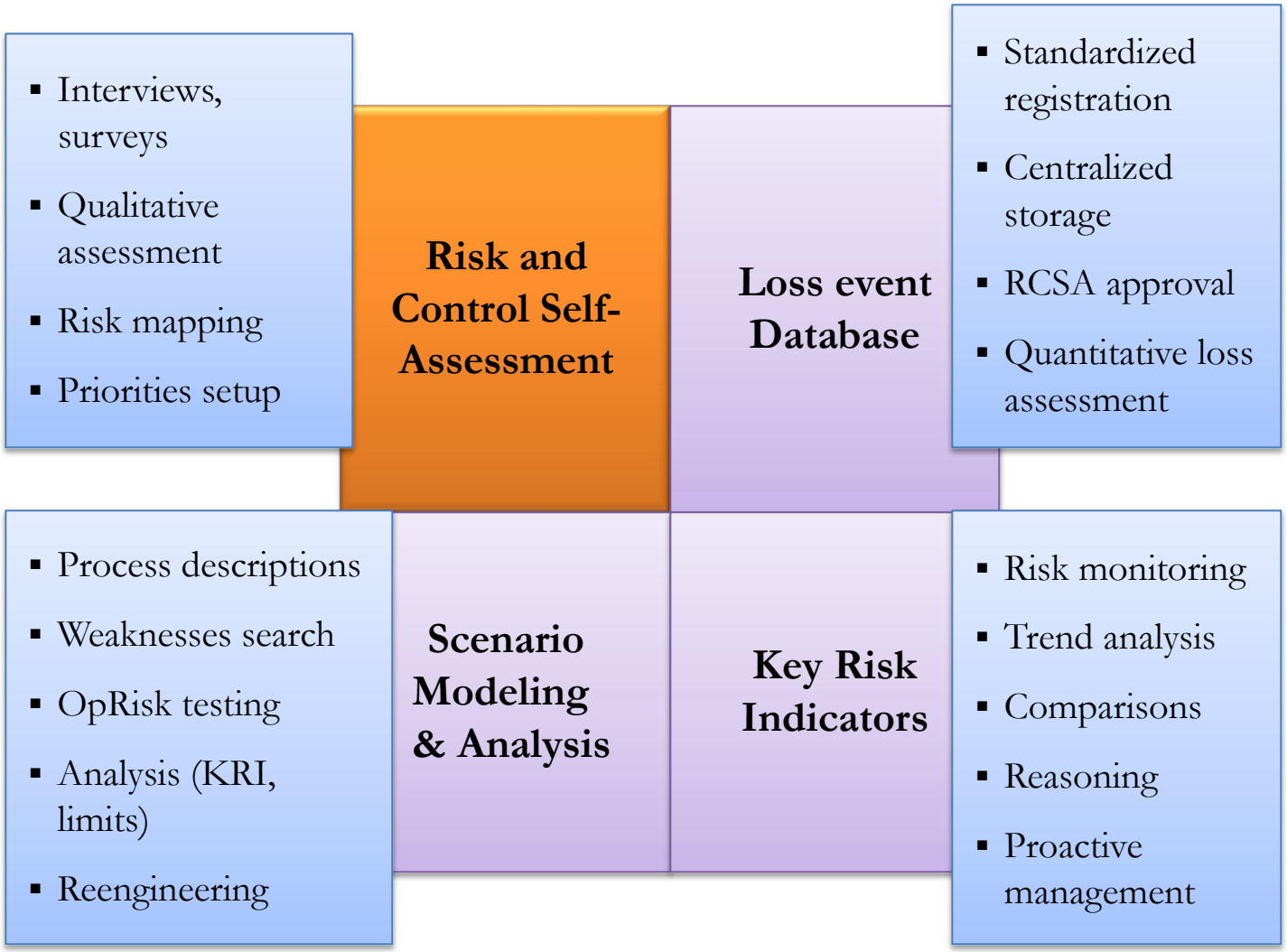
Risk transfer through insurance

Table of Contents

Table of Contents

Pillar I. Identification Tools

MAIN OPERATIONAL RISK MANAGEMENT TOOLS



RCSA: PROACTIVE RISK IDENTIFICATION & MANAGEMENT TOOL

Basel 2 AMA requirement under **business factors internal and control environment**: —Bank should identify the OpRisk inherent in all types of products, activities, processes and systems‖.

Allows to coordinate / **integrate** the risk identification and management.

5 **aspects** to consider

- ✔Focus
- ✔Timing
- ✔Ownership
- ✔Reporting
- ✔Continuity

- Business lines & support functions risks & assess controls in their area;
- RCSA provides systematic means to identify
  - Risk clusters (concentrations),
  - Control duplications / gaps or over-controls

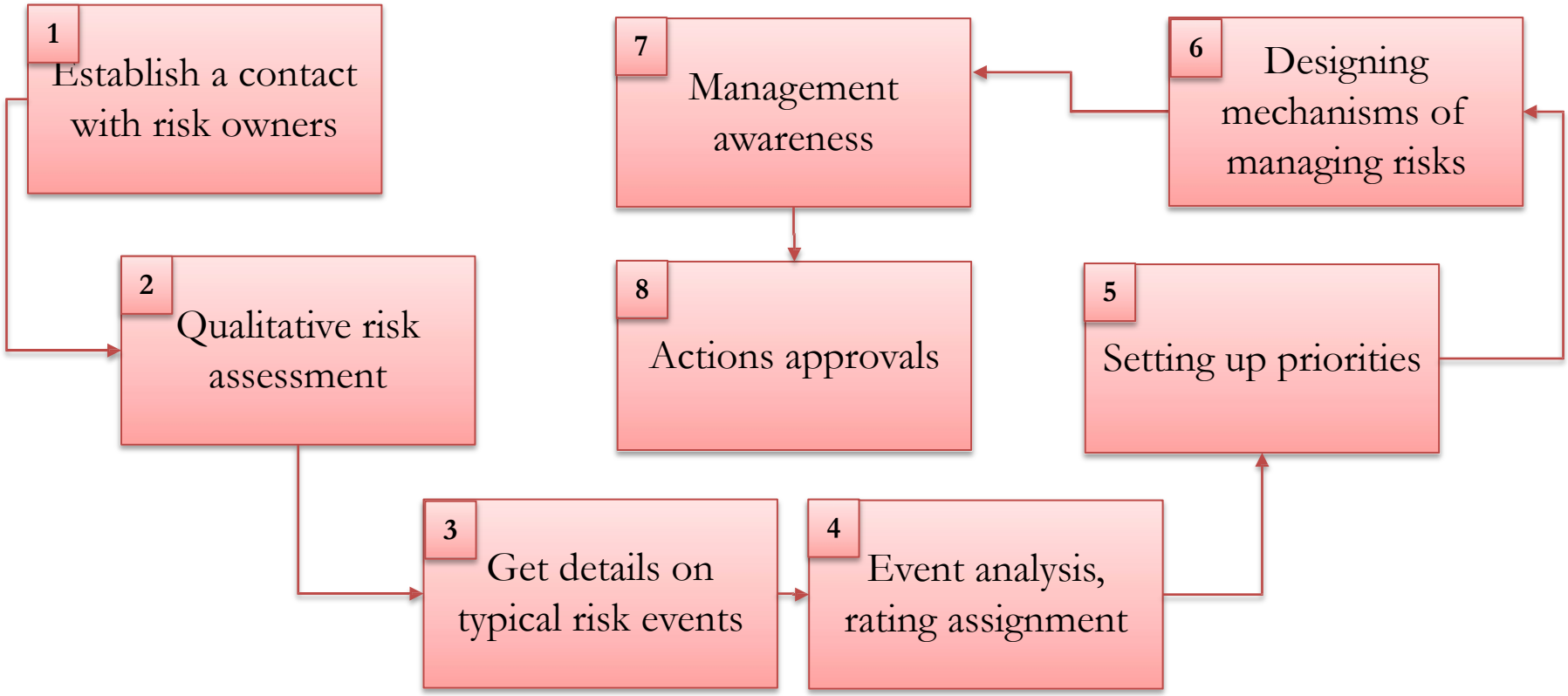
and to set up:

- prevention & control measures and
- corrective action plans;

- Original **Internal Audit tool**, facilitates a risk-focused approach to Internal Audit;
- Complimentary **Management Tool**, generally accepted to satisfy corporate governance & regulatory requirements.
- RCSA **proactive** as opposed to Op Loss Reporting
- Allocates front line responsibility for ORM and place control directly with management – hence, corrective actions more effective & timely;
- Creates a cultural change in the institution

RCSA AIMS

RCSA **aims** at:
-identifying OpRisks;
-assessing (incl. quantifying) the institution‘s exposure to OpRisks;
-evaluating the prevention & control system; and
-mitigating the risks



RCSA MILESTONES

Define Business Objectives / Risk Tolerance / Appetite (as to residual risk)

Identify & Evaluate the Intrinsic OpRisks / Risk Drivers of each activity and Institution's Risk Profile

Naturally inherent risks, —net‖ of the prevention & control environment

Evaluate the quality of Existing Prevention & Control Systems, enabling Risk Reduction

the existence & ef-(de)fectiveness of systems of detecting and preventing risks and/or their capacity to reduce the financial impact and responsibility for controls (NB! **excessive controls & their re-allocation**)

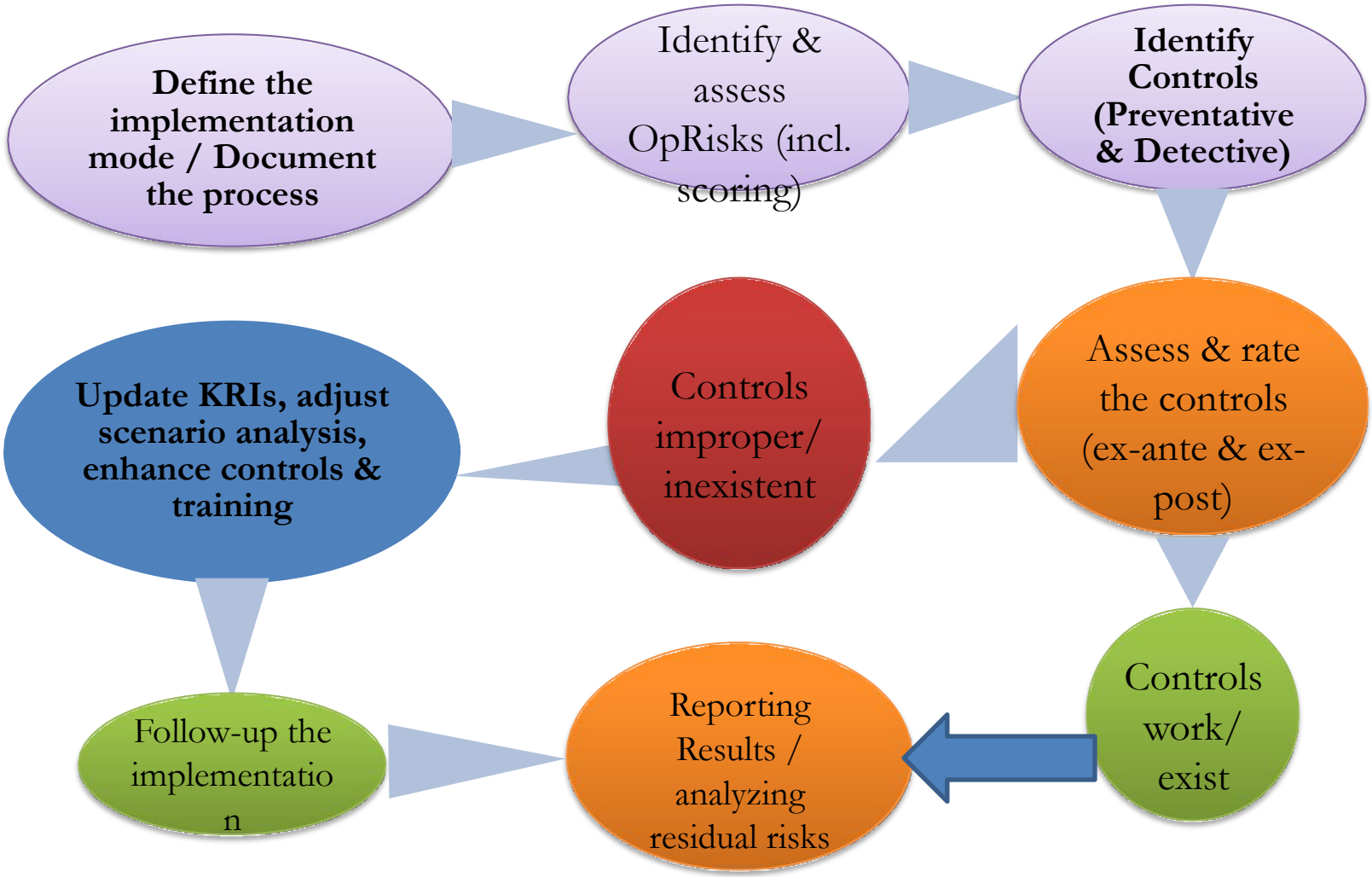
Reduce Exposure to Residual OpRisks of each activity

after counting the prevention & control environment, excl. insurance

Corrective Action Plans / Risk Mitigation Plans (RMPs)

RCSA outputs risk/reward judgments

RCSA WORKFLOW



RCSA TOOLKIT-3: OpRisk MAPPING

Used for process risk analysis

Risk register (*also for output*)

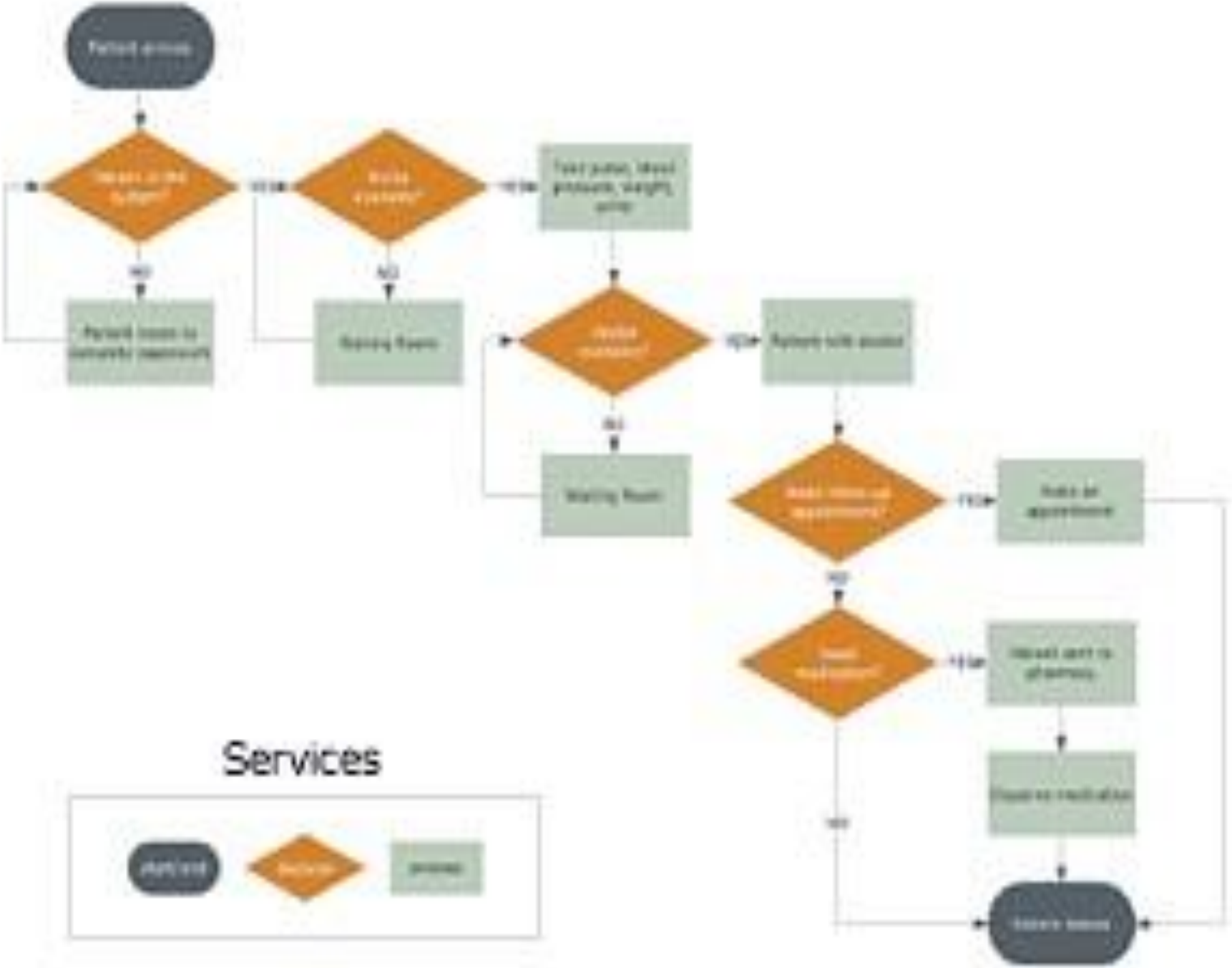
- High level business process (e.g. HR Mngt)
- Bank sub-process/task (e.g. hiring)
- Specific risks (e.g. hiring crooks), can be mapped to multiple categories

Org Level Risk Map as per organizational unit (risk owner)

- Process
- Sub-process
- Risk
- Control / Mitigant (general/specific)
  - documented?
  - manual/system?
  - line/independent?
  - Frequency?

Determine risks not identified in the repository;

Implant SOFT CONTROLS (communication, degree of trust to managers, aware of procedure, mgnt style; ethics)


Services

INPUT OpRisk MAPPING SAMPLE

Governance	Integrity	Compliance
▪ Authority ▪ Leadership ▪ Performance ▪ Incentives ▪ Limits	▪ Management Fraud ▪ Employee Fraud ▪ Illegal Acts ▪ Unauthorized Use	▪ Federal Banking Regulations ▪ Taxation ▪ Pension Fund ▪ Bank Secrecy Act ▪ Ethics and Control Framework ▪ Risk Management Framework

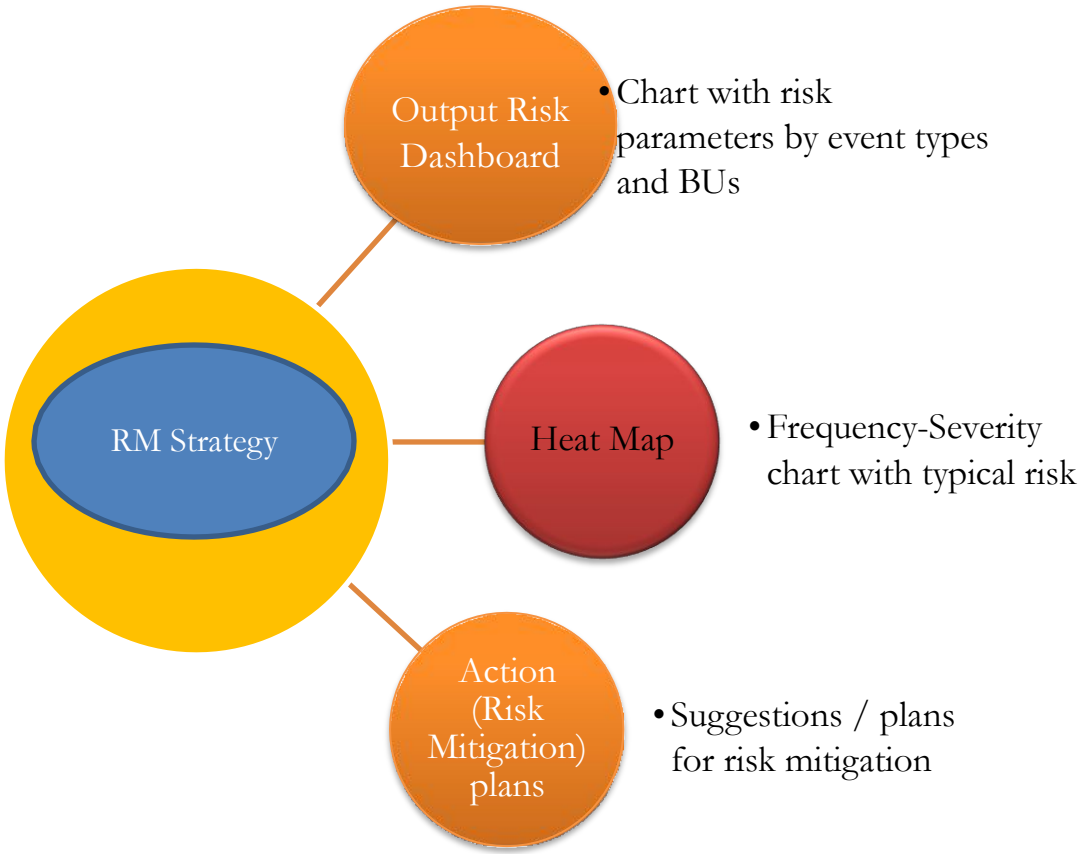
Business Processes			
▪ Technology ▪ New Product Development ▪ Customer Satisfaction ▪ Credit Quality ▪ Deposit Operations	▪ Funds Transfer ▪ Items Processing ▪ Acquisitions ▪ Business Integration ▪ Marketing ▪ Efficiency	▪ Business Continuity Planning ▪ Operations Support Management ▪ Capital Expenditures ▪ Performance Management	▪ HR Competencies ▪ Motivation ▪ Training ▪ Security Systems

Information Management	Financial Management	Human Resources
▪ Management Information Systems ▪ Dependence on IT ▪ Reliability and Security ▪ E-Commerce ▪ Access/Availability ▪ Completeness/Assurance ▪ Relevance	▪ Budgeting & Planning ▪ Portfolio Management ▪ Investment Evaluation ▪ Financial Reporting ▪ Financial Instruments /Trading ▪ Funding ▪ Accounting Information	▪ HR Management ▪ Competencies ▪ Recruitment ▪ Recognition/Retention/ Compensation ▪ Performance Management ▪ Leadership Development

MANAGEMENT RESULTS REPORTIG TOOLS

Unless RCSA results are relevant for management decision making, the exercise is no more than an expensive awareness tool

Mngt Reporting thru:
dashboards / heat maps / scorecards



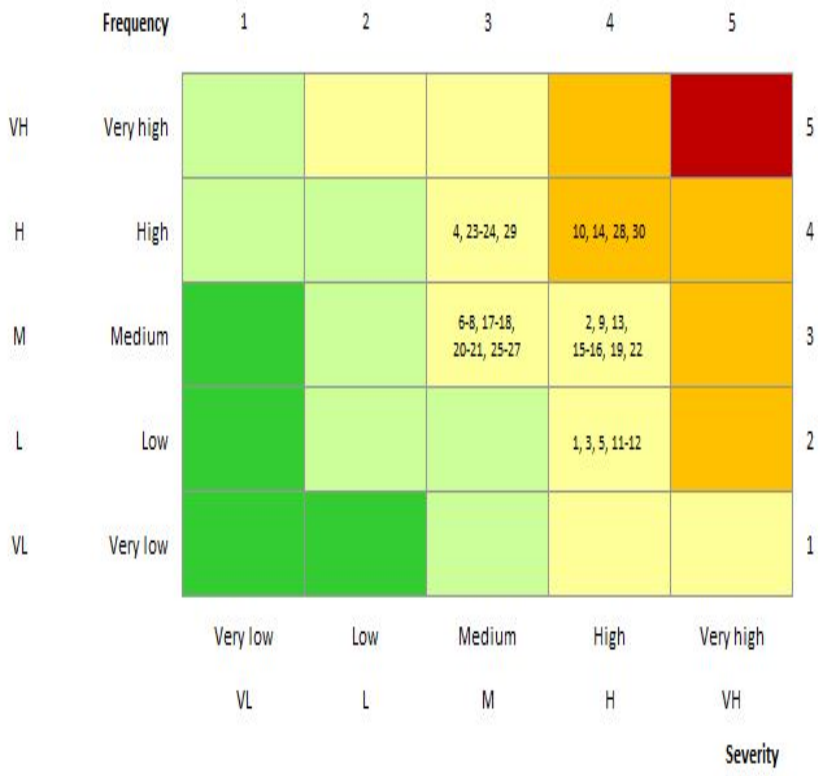
OUTPUT RISK SCORECARD

Business uinits	Sources of OpRisk							
	People		Processes			Systems	External	
	Types of OpRisk events							TOTAL
	Internal Fraud (1)	External Fraud (2)	Execution, Delivery & Process Management (7)	Clients, Products & Business Practices (4)	Employment Practices and Workplace Safety (3)	Business Disruption and System Failures (6)	Damage to Physical Assets (5)	
Management				H	H			H
Front-office	H	M	M	H				M
Middle-office			M					M
Back-office	H	H	M	M				M
Treasury				M				M
IT department		VH	M			H		H
Legal department			H	M				M
Security department	M	H					H	M
Administration			M		L	H	H	M
Accounting	H		H		L			M
Human Resources	M		H		L			M
TOTAL	H	H	M	M	M	H	H	M

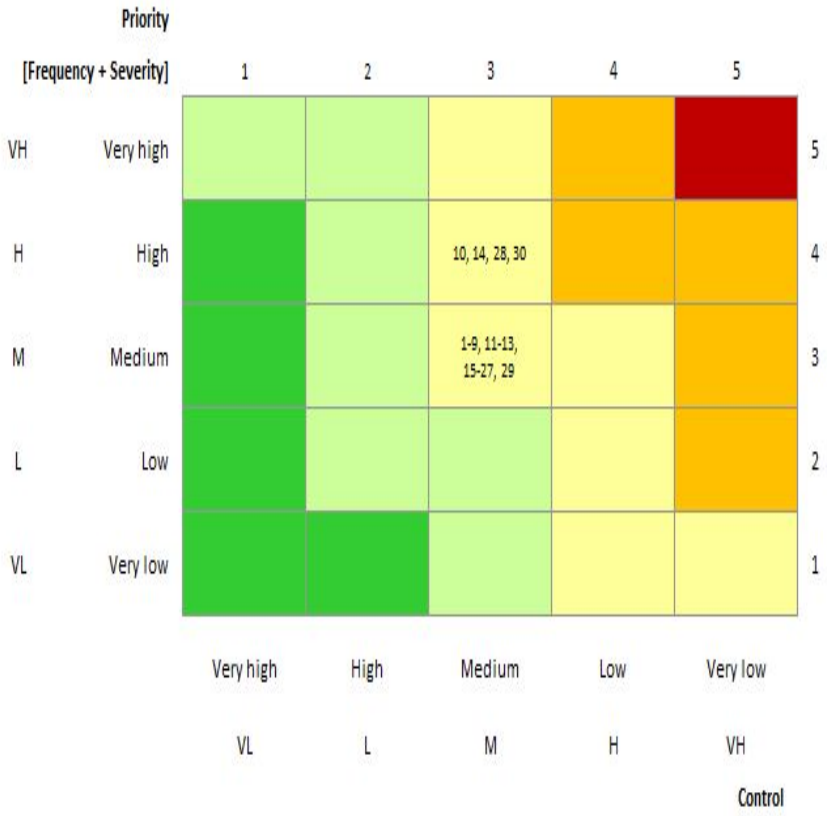
HEAT MAPPING

facilitates the assessment of the likelihood and impact of the risk materializing; Can also be used to help determining the "top" risks

Frequency-Severity Matrix



Frequency-Severity-Control Matrix

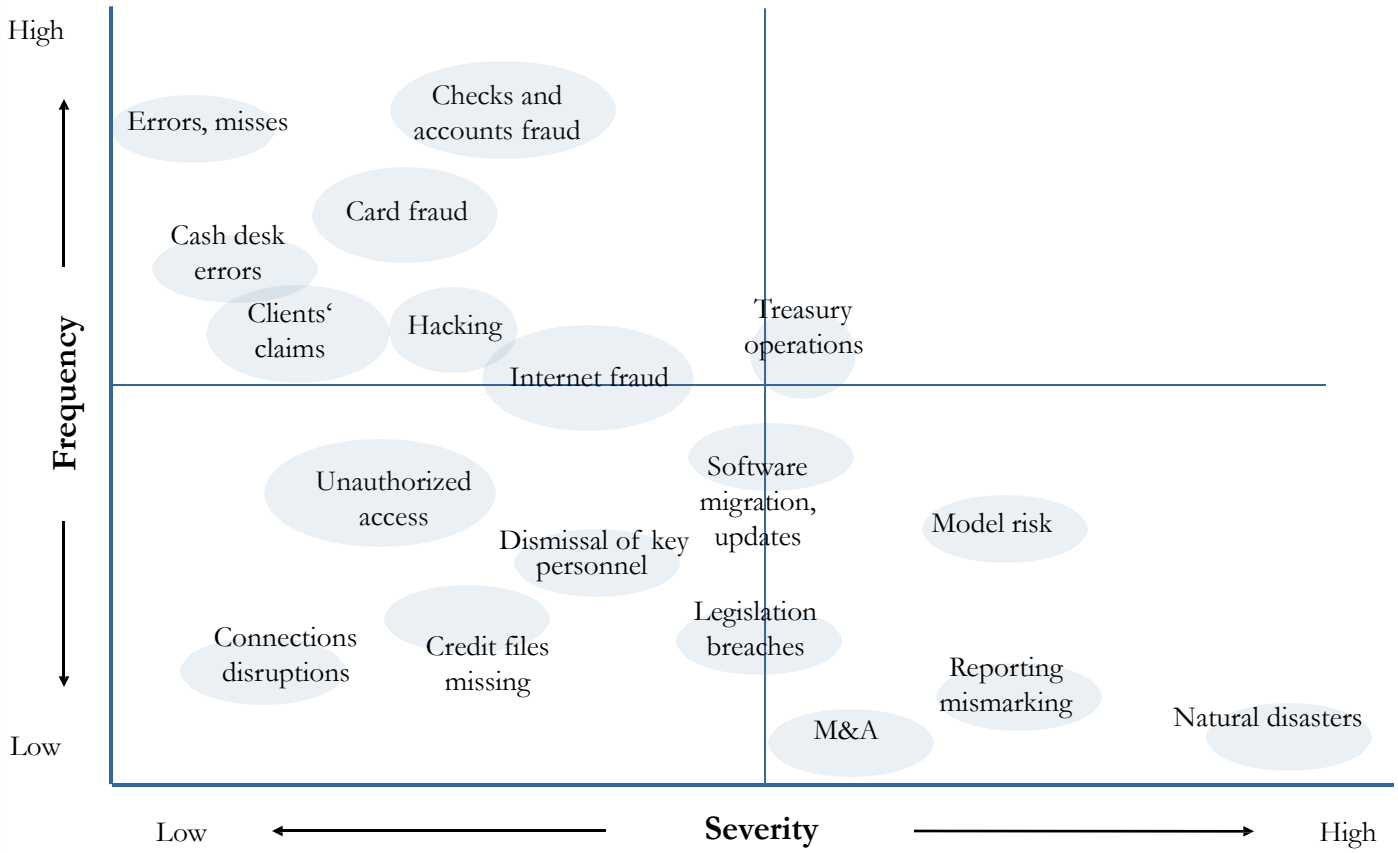


OPERATIONAL FREQUENCY – SEVERITY RISK MAPPING

Score Card

Bank must determine a scoring system to quantify / express:

- Intrinsic (initial) risk
- Effectiveness (rating) of controls
- Losses and their frequency expected (given current controls)
- Residual risk (taking above 3 into account)



RCSA FOLLOW UP

RCSA results ought to be used **in conjunction with other components** of ORM Framework.

Internal Event Data:

-Highlight areas susceptible to OpRisk loss events;

-Reassures quality of RCSA

External loss data

-RCSA Identifies areas of vulnerability that may benefit from considering fast-track external data;

-Data helps determining potential weaknesses / inherent risks for RCSA

Scenario analysis

-RCSA results serve a valuable input source;

-Defining risk scenarios leads to identifying risk factors failed to be captured within RCSA.

Timing / Frequencies of further RCSA exercise

-Annual for key processes;
-More frequent for high risk areas;
-Following major changes (e.g. after a merger).
NB! End before annual budgeting process.

Table of Contents

Pillar I. Identification Tools

SOUND PRACTICE

Basel Committee on Banking Supervision
Principles for the Sound Management of Operational Risk, June 2011

Indicators approach is listed as an example of tools that may be used for identifying and assessing operational risk:

—Risk and performance indicators are risk metrics and/or statistics that **provide insight into a bank's risk exposure**. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are **often paired with escalation triggers** to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans‖

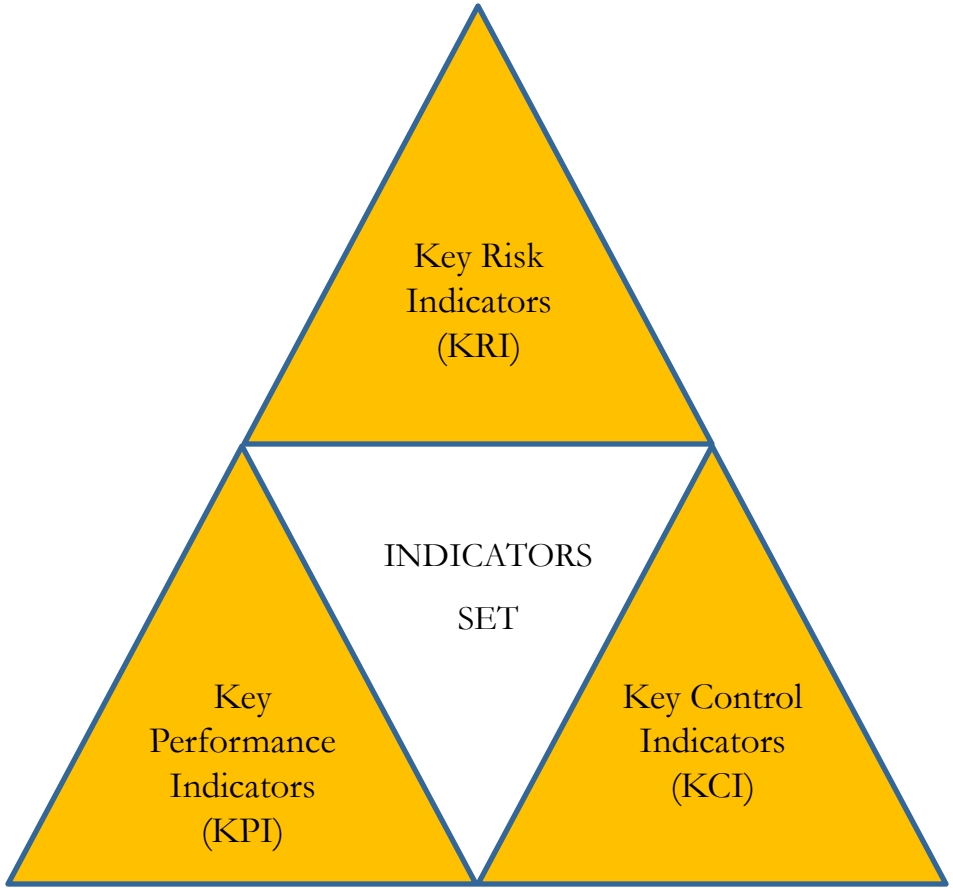
LET FIGURES TALK

Indicators Approach allows to track operational risk profile and monitor risk exposure with series of quantitative measures describing certain risk areas, scale of operations and control procedures

Best use:

- Quantitative analysis while no risk event collection
- Early check up and qualitative projections
- Benchmarking of risk owners
- Targeted decision-making
- Validation of other identification tools

INDICATORS COMPOSITION and DATA SOURCES



KEY RISK INDICATORS (1/2)

KRIs are the measures summarizing the frequency, severity and impact of OpRisk risk events or corporate actions occurred in the company during a reporting period

Risk dimension	Indicators type
Frequency	▪ Number of risk events
Severity	▪ Volume of risk events ▪ Average risk losses ▪ Maximum duration of disruptions
Impact	▪ Total amount of risk losses ▪ Cost of mitigations

KEY RISK INDICATORS (2/2)

Branch network • Number of complaints and claims to the company • Number of lost clients • Amount of compensation paid to the client • Volume of balances lost / opportunity cost	**Loan / Client department** • Average days of getting loan approval • Number of identified fraud cases • Client dissatisfaction evidenced by client surveys • Number of critical errors detected in credit files
Legal department • Number of legal actions against the company / third parties • Volume of legal actions against the company / third parties • Number of regulatory enquires / legislation breaches	**Finance department** • Volume of penalties, imposed by regulators • Total amount of suspicious transactions • Number of late completion or non-completed transactions
Human resources • Turnover of experienced staff • Number of temporary/short term staff • Number of employees, attended training courses • Number of employees, failed to pass mandatory evaluation	**IT** • Number of failures related to IT system and other equipment • Number of calls to help desk on IT system and other equipment • Average down-time of IT system and other equipment • Increase in transaction load on systems

KEY PERFORMANCE INDICATORS

KPIs are the measures that evaluate scale of banking activities. According to many empirical observations that is directly related to operational risk exposure

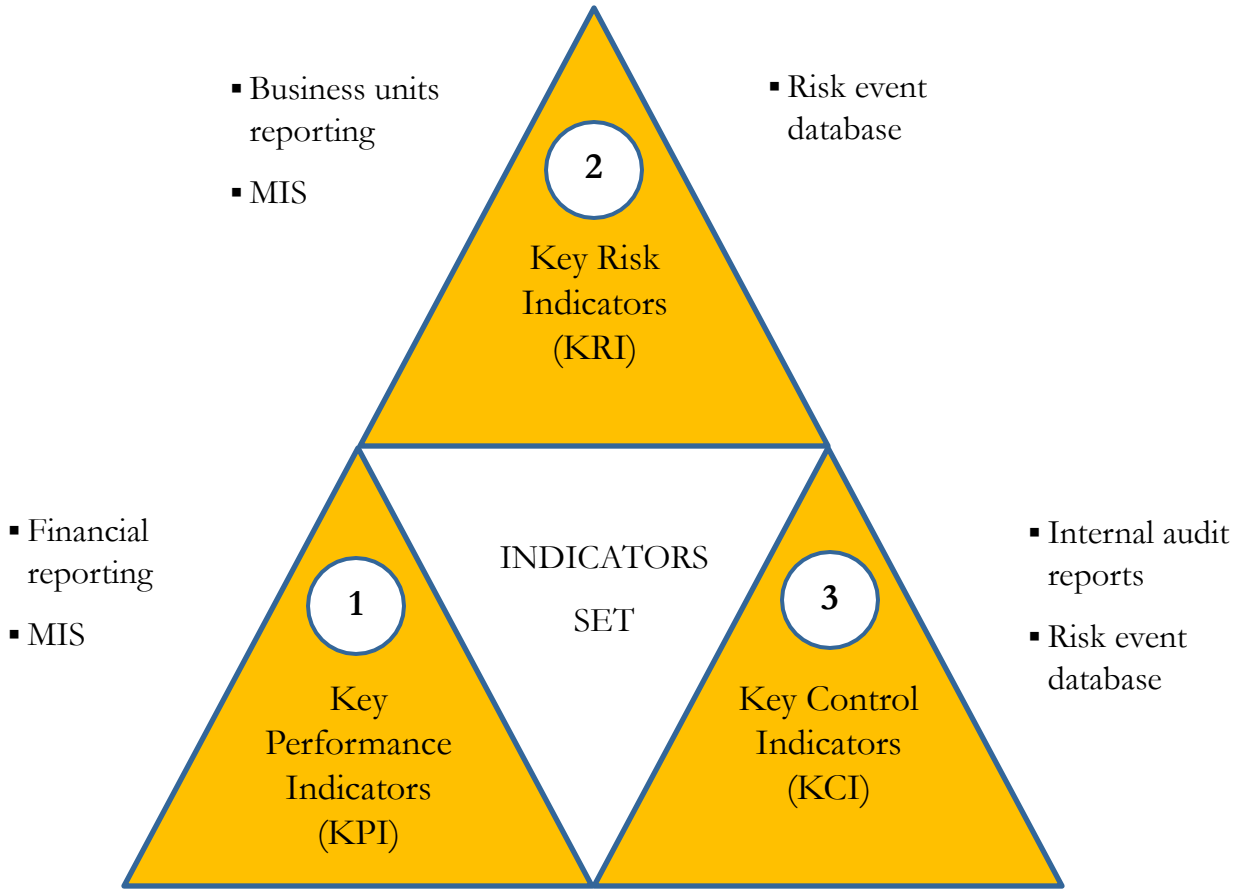
Extension Risk	**People Risk**
• Gross Income	• Number of Employees
• Total Assets	• Staff Payroll
• Book Value of Fixed Assets	• Income per Employee
• Cost to Income	• Cost per Employee
Customer / Reputational Risk	**Process Risk**
• Number of client accounts	• Volume of transactions
• Volume of client accounts	• Number of transactions
• Average balance of single client account	• Average amount of single transaction

KEY CONTROL INDICATORS

KCIs are the measures that enables to monitor effectiveness of OpRisk management procedures established in the company, collected from business units, Risk management, Internal Audit reports, and Regulators

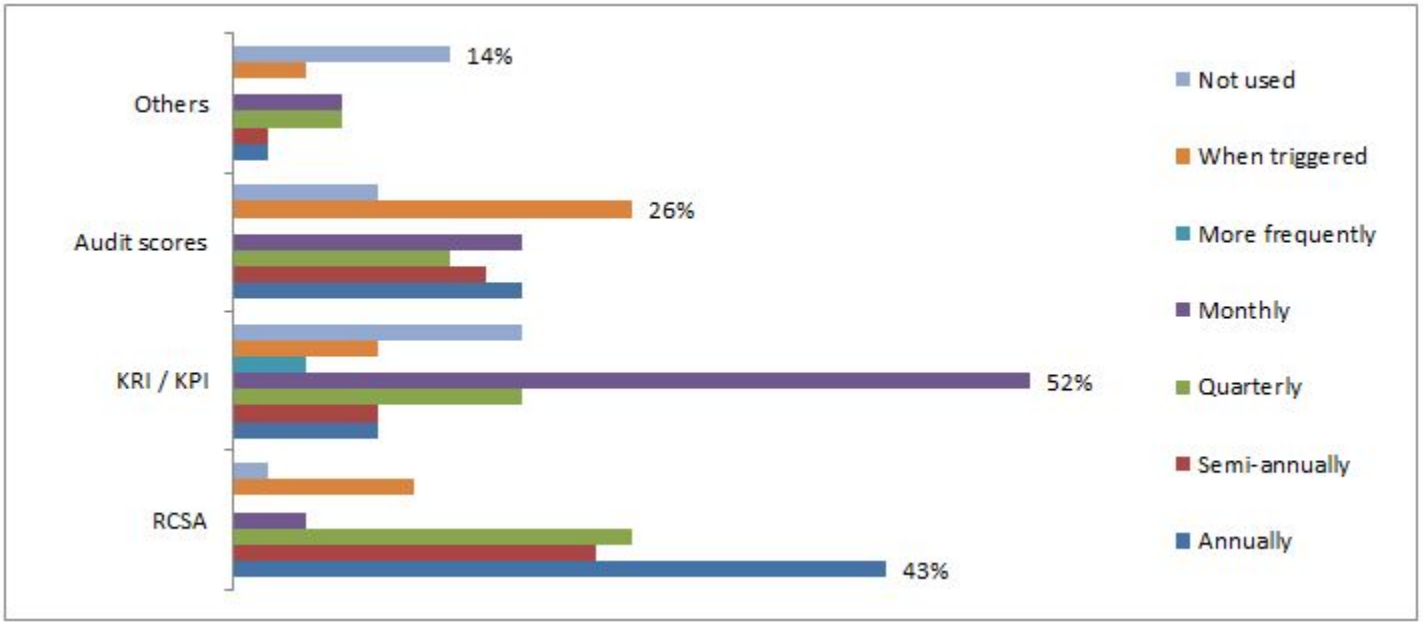
Business Units	**Risk management**
• Number of breaches identified by the staff • Number of disciplinary actions taken • Percentage of loss mitigation	• Number of days before breaches are identified • Number of action plans introduced • Number of action plans failed to implement
Internal Audit	**Regulators**
• Number of breaches in processes identified by internal audit • Number of breaches eliminated	• Number of claims on the company in the area of OpRisk made by the regulator • Number of errors eliminated

DATA SOURCES



DATA COLLECTION FREQUENCY

Medium bank updates KRIs/KPIs more frequently, than other identification tools, typically on monthly and rarely quarterly time periods



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

DATA ANALYSIS (1/2)

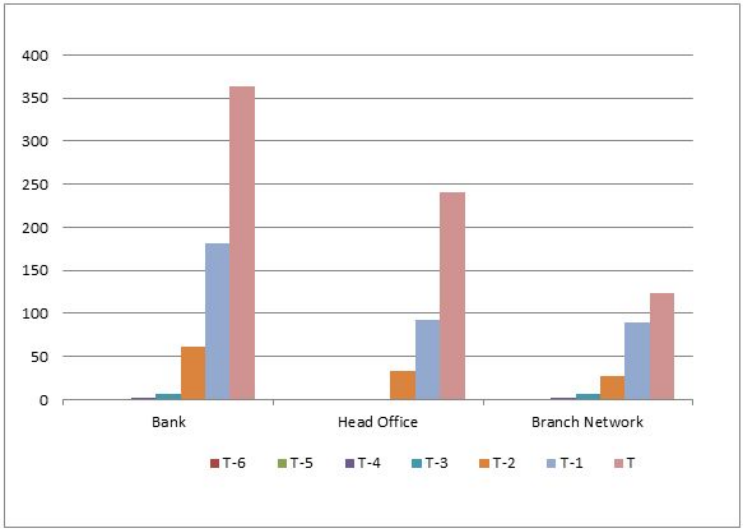
DATA BREAKDOWNS

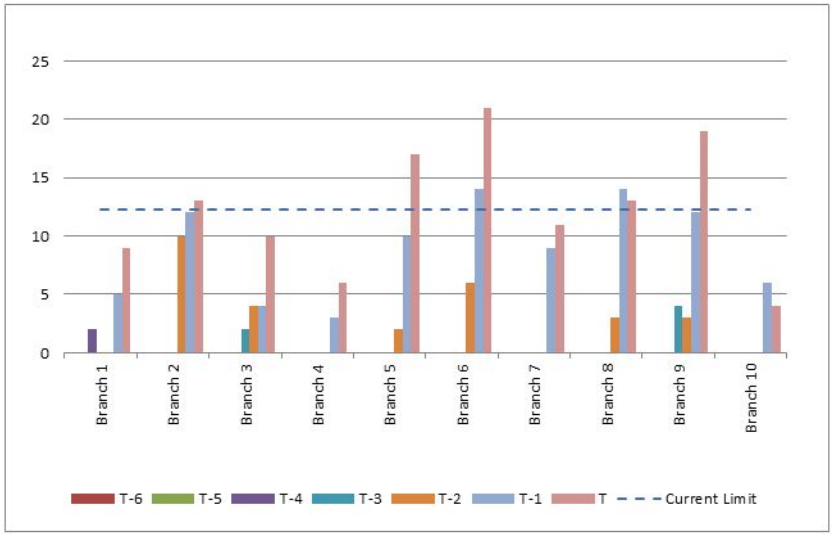
Upright

- Peers
- All bank
- Headquarter
- Branch network

Horizontal

- Business lines
- Departments
- Branches





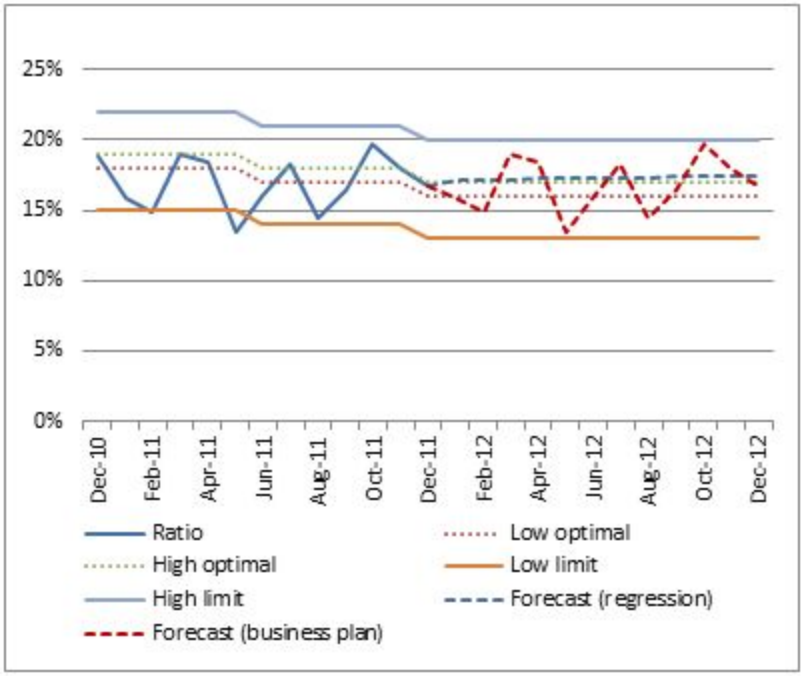
DATA ANALYSIS (2/2)

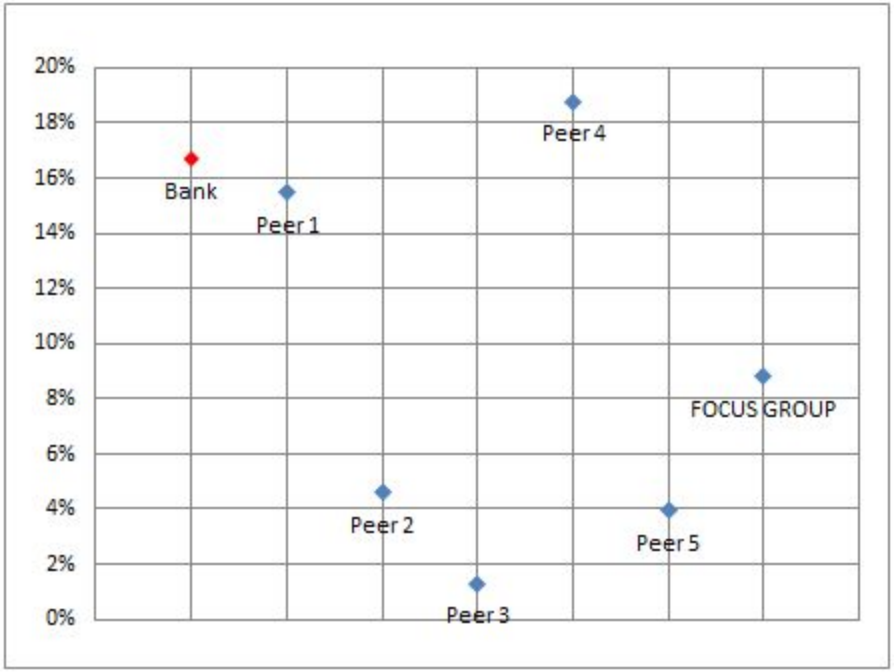
Trend analysis

- Retrospective
- Business plan
- Regressions
- Peers KPI comparison

Thresholds Control

- Peers line
- Average (optimal)
- Alarm levels (STD)
- Limits (exceptions)
- Risk Class





REPORTING MATRIX

Reporting Area	Frequency	Risk Owner	Risk Man	Audit	OR Com	MB
Risk indicators collection	•Monthly	R	C	-	-	-
	•Quarterly	R	C	R	-	-
	•Annually	-	-	R	-	-
Retrospective indicators / Regression forecasts / Thresholds check	•Monthly	I	R	-	I	-
	•Quarterly	-	-	I	I	I
Business plan indicators / Thresholds check	•Quarterly	-	R	I	I	I
Peers Comparison / Thresholds check	•Quarterly	-	R	I	I	I
	•Annually	-	R	I	I	I

DECISION MAKING MATRIX

Observations	Decision Making Options	Risk Owner	Risk Man	Audit	OR Com
Sudden outliers (Risk Class = Watch)	•Contact risk owner •Find out the reason •Put the risk owner in a watch list	- R -	C C R	- - -	- - I/A
Negative tendency (Risk Class = 1)	•Prepare action plan •Approve and monitor the plan •Set thresholds	R - -	C R R	- - -	- I/A A
Alarm threshold breach (Risk Class = 2)	•Written explanation of the breach •Activate contingency plan	R -	C R	- -	- I/A
Limit overriding (Risk Class = 3)	•Issue a summons to ORCom •Make unplanned audit inspection	R -	R R	- I/C	I/C -

Table of Contents

Pillar I. Identification Tools

SOUND PRACTICE (1/2)

Basel Committee on Banking Supervision
Principles for the Sound Management of Operational Risk, June 2011

Business Process Mapping is listed as an example of tools that may be used for identifying and assessing operational risk:

—Business process mappings **identify the key steps** in business processes, activities and organisational functions. They also identify the key **risk points** in the overall business process. Process maps can **reveal individual risks, risk interdependencies, and areas of control or risk management weakness**. They also can **help prioritise subsequent management action**.‖

Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk

SOUND PRACTICE (2/2)

The review and approval process should consider:

a) inherent risks in the new product, service, or activity

b) changes to the company's operational risk profile and appetite and tolerance, including the risk of existing products or activities

c) the necessary controls, risk management processes, and risk mitigation strategies

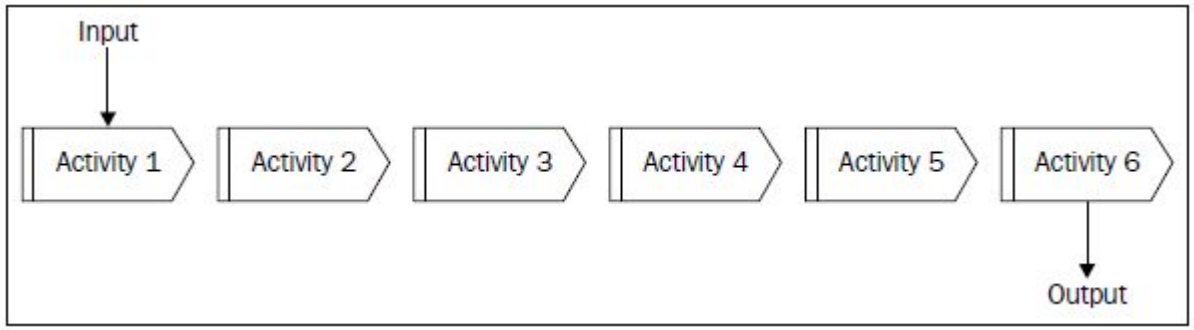
d) the residual risk

e) changes to relevant risk thresholds or limits

f) the procedures and metrics to measure, monitor, and manage the risk of the new product or activity

DIVE IN PROCESSES

Business process is a collection of linked activities that consume inputs, add value, and produce an output of value to an internal or external customer

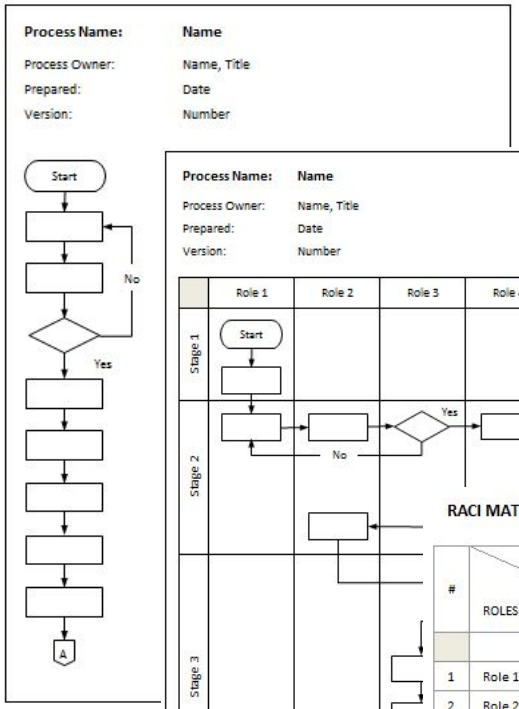


Process risk is the type of operational risk arisen from inadequate or improper internal business processes in the companys and lack of built-in control mechanisms

BUSINESS PROCESS MANAGEMENT TOOLS

Process engineering

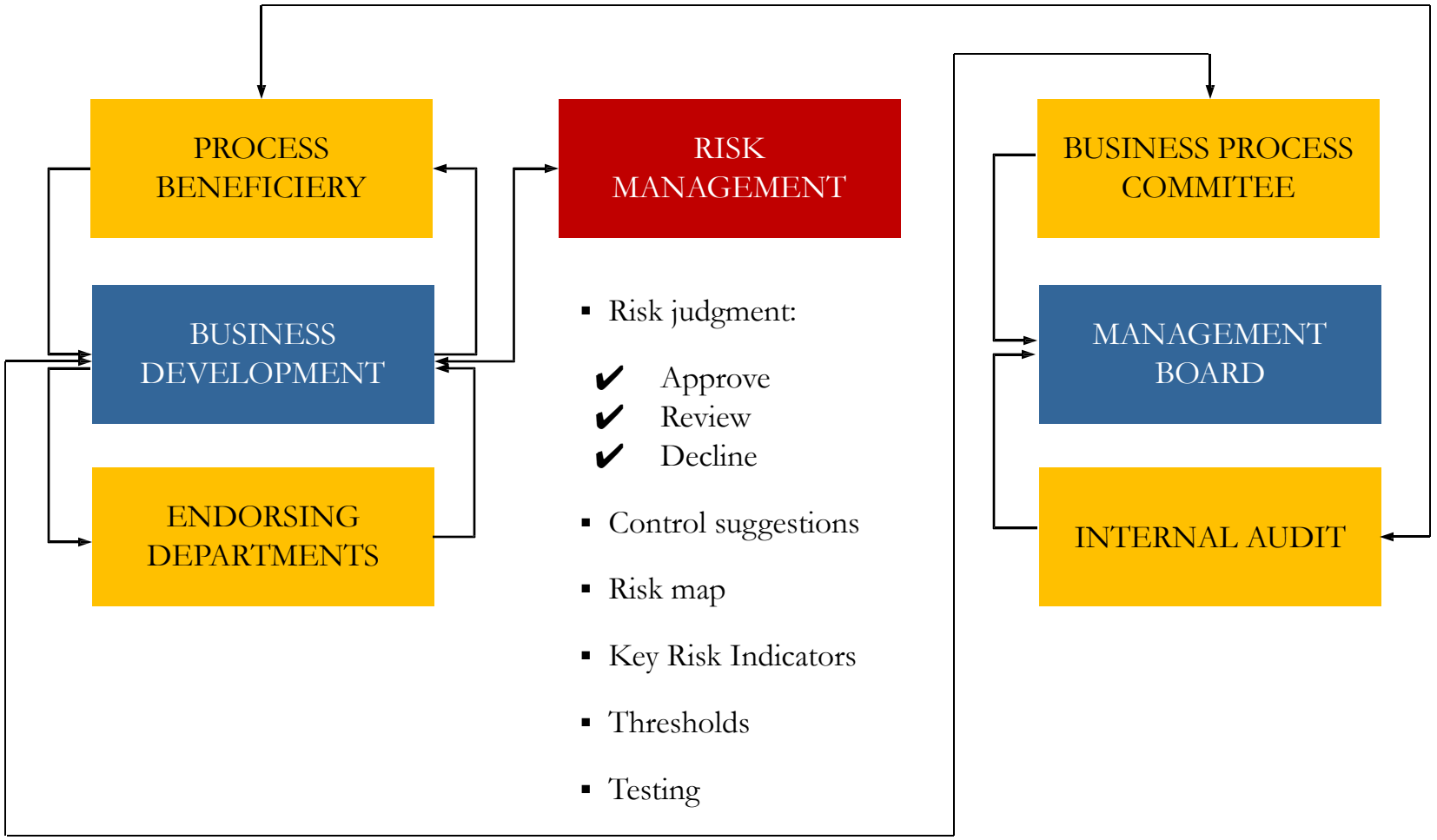
- ❑ Process initiation document
- ❑ As Is:
  - Flowchart
  - Activity flow diagram
  - RACI matrix
  - Process metrics analysis
- ❑ To Be:
  - Activity flow diagram
  - RACI matrix
  - Implementation plan



RACI MATRIX

#	ROLES \ PROCESS STEPS	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10
	Index	1	2	3	4	5	6	7	8	9	10
1	Role 1	R	R			R				I	
2	Role 2	I	I	C	R	I	C	R		I	
3	Role 3	I									
4	Role 4	I	I	A							
5	Role 5					I	A	A			
6	Role 6					I			R		
7	Role 7	I	I		I				C	R	C
8	Role 8	I			I				I		
9	Role 9				I				I	I	
10	Role 10				I				A		A

HOW RISK MANAGEMENT SIGN OFF THE PROCESS?



PROCESS RISK MAP

Process risk map is composed and monitored by Risk management on the basis of key workflows with the idea to identify and control inherent OpRisks

High priority risks should be mitigated before the new process is launched

#	Process Stage	Risk ID	Risk Type	Risk description	Risk origin	Potential effects	Mitigants implemented	Mitigants to be introduced	Risk priority	Indicators ID	Key Indicators
1	Client application	R1|1	Misseling	Client is wrongly advised about terms of the cash loan or other products	Lack of training	Operation refuse, loss of clients	Supervisor check	Mystery shopping	Medium	I1	Client complaints
2	Screening	R2|1	Documents incomplete	Officer overlooks documents supporting application	Staff turnover Large workload	Lower recovery	Supervisor check Audit inspection	Penalties	Medium	I2	Audit conrols
3	Cut-offs check	R3|1	Client forgery	Client compromises the documents to get approval	Business risk	Bad loans	Verification process	Vintage analysis	High	I3	Fraud detections
4	Qualitative judgement	R4|1	Internal credit fraud	Officer improve borrower credentials to his friends or relatives	Bad business culture	Bad loans	Report of conflict of interest	Warning list that includes relatives	Low	I4	Fraud detections
5	Data uploading	R5|1	Data error	Officer	Negligence Large workload	Lower recovery	Verification process	Automatic checks of IT system	Low	I5	Data errors

RISK CONTRIBUTION TO FLOWCHART

Quality controls make the flowchart telling what goes wrong or well in business process

Risk controls

- Risk qualitativ e judgment
- Risk and Control indicators
- Areas of comfort / concern
- Timeline: gross and by operations

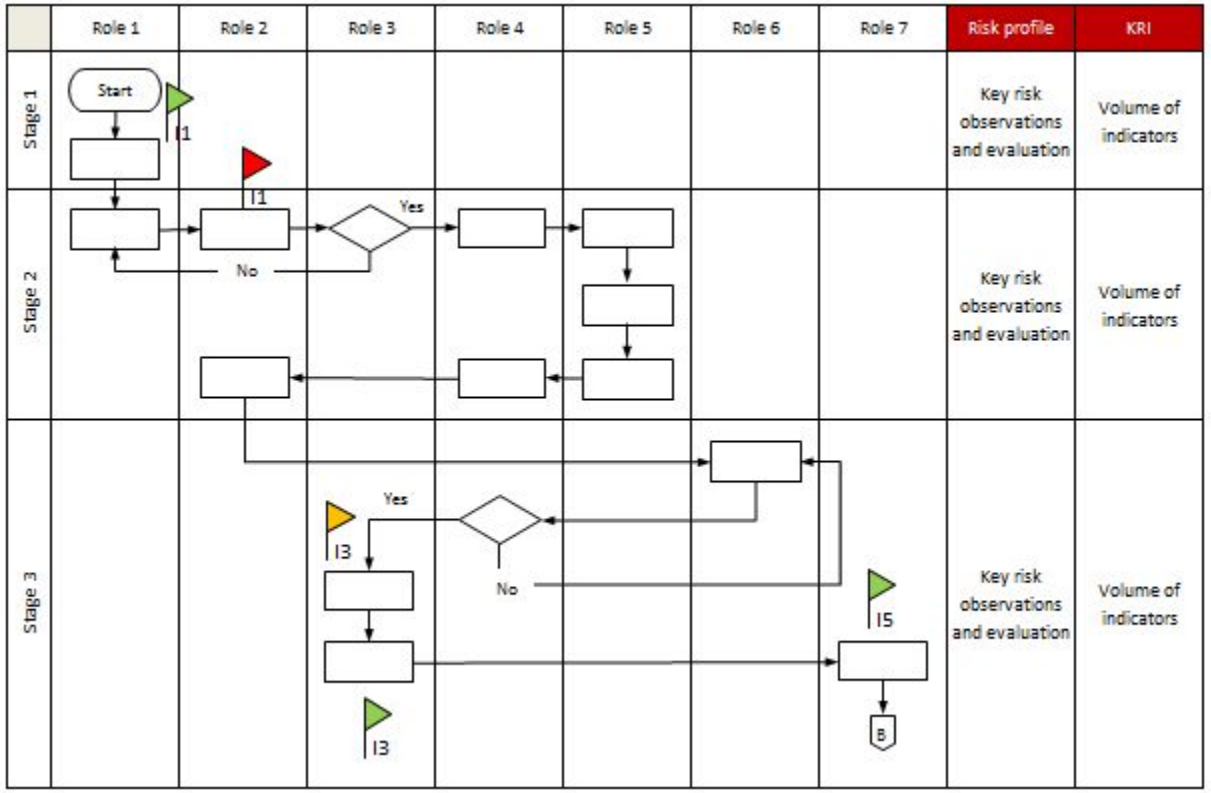


Table of Contents

Table of Contents

Pillar II. Risk Measurement and Analysis

SOUND PRACTICE

Basel Committee on Banking Supervision
Principles for the Sound Management of Operational Risk, June 2011

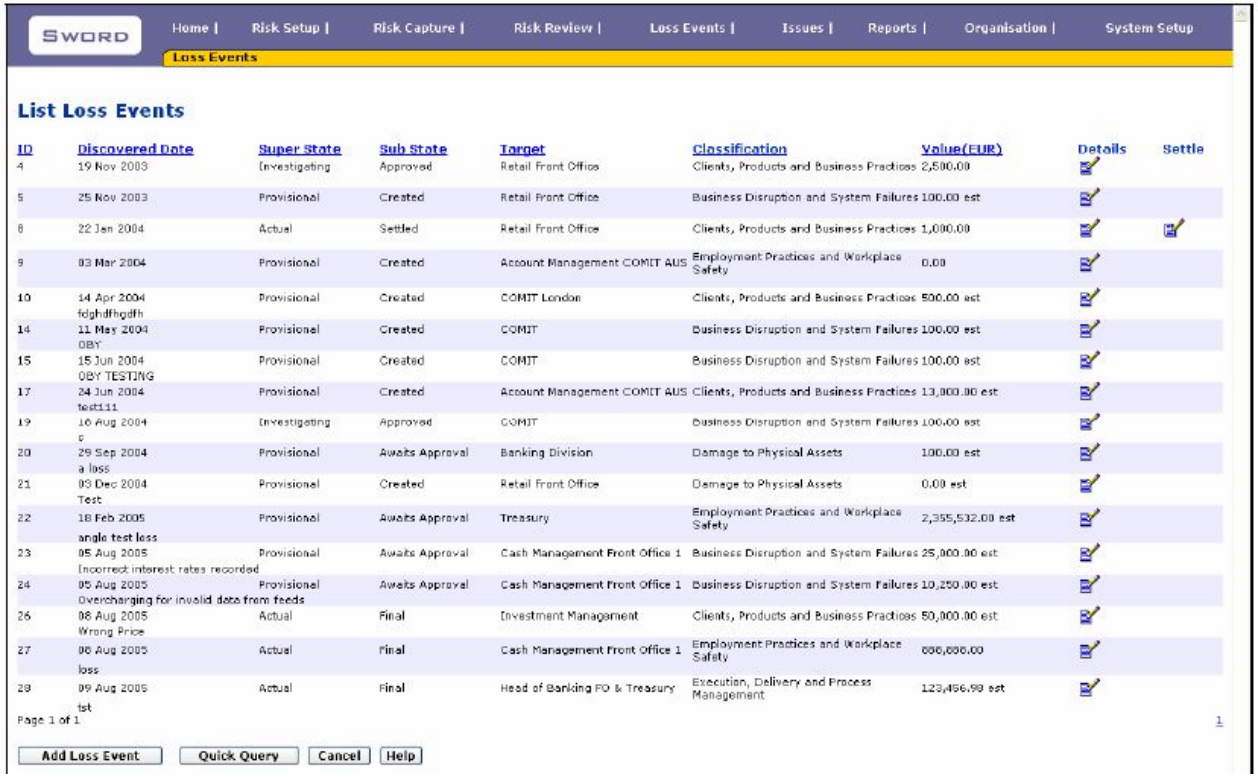
Loss data collection is listed as an example of tools that may be used for identifying and assessing operational risk:

— Internal Loss Data Collection and Analysis: Internal operational loss data provides meaningful information for **assessing a bank's exposure to operational risk and the effectiveness of internal controls**. Analysis of loss events can **provide insight into the causes of large losses** and information on whether control failures are isolated or systematic.‖

—External Data Collection and Analysis: External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organisations other than the company. External loss data can be **compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures**‖

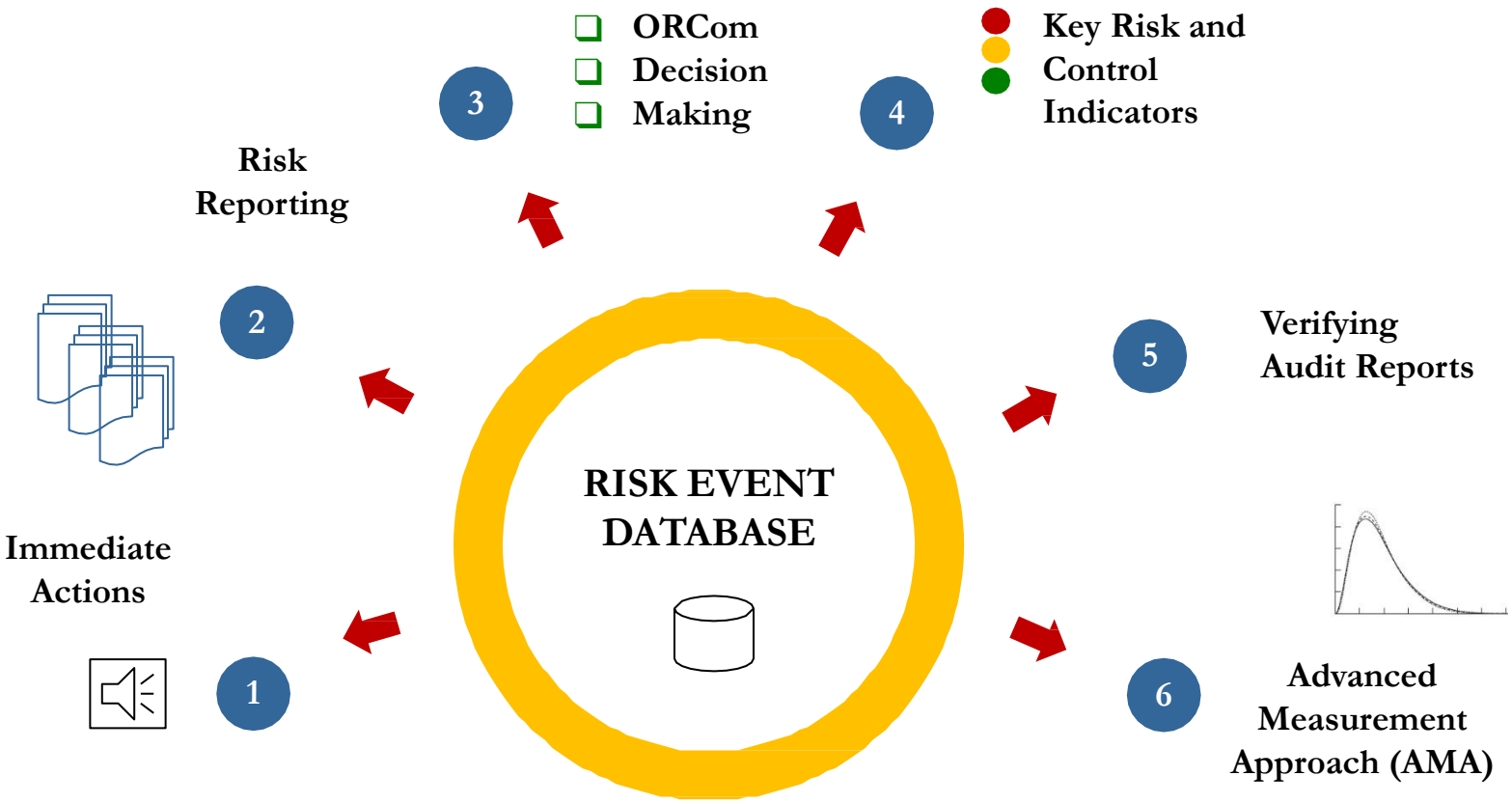
RISK EVENT DATA COLLECTION

Risk event database is a register of risk event records that enables to accumulate, classify, keep and export data relevant to observed internal and external risk events

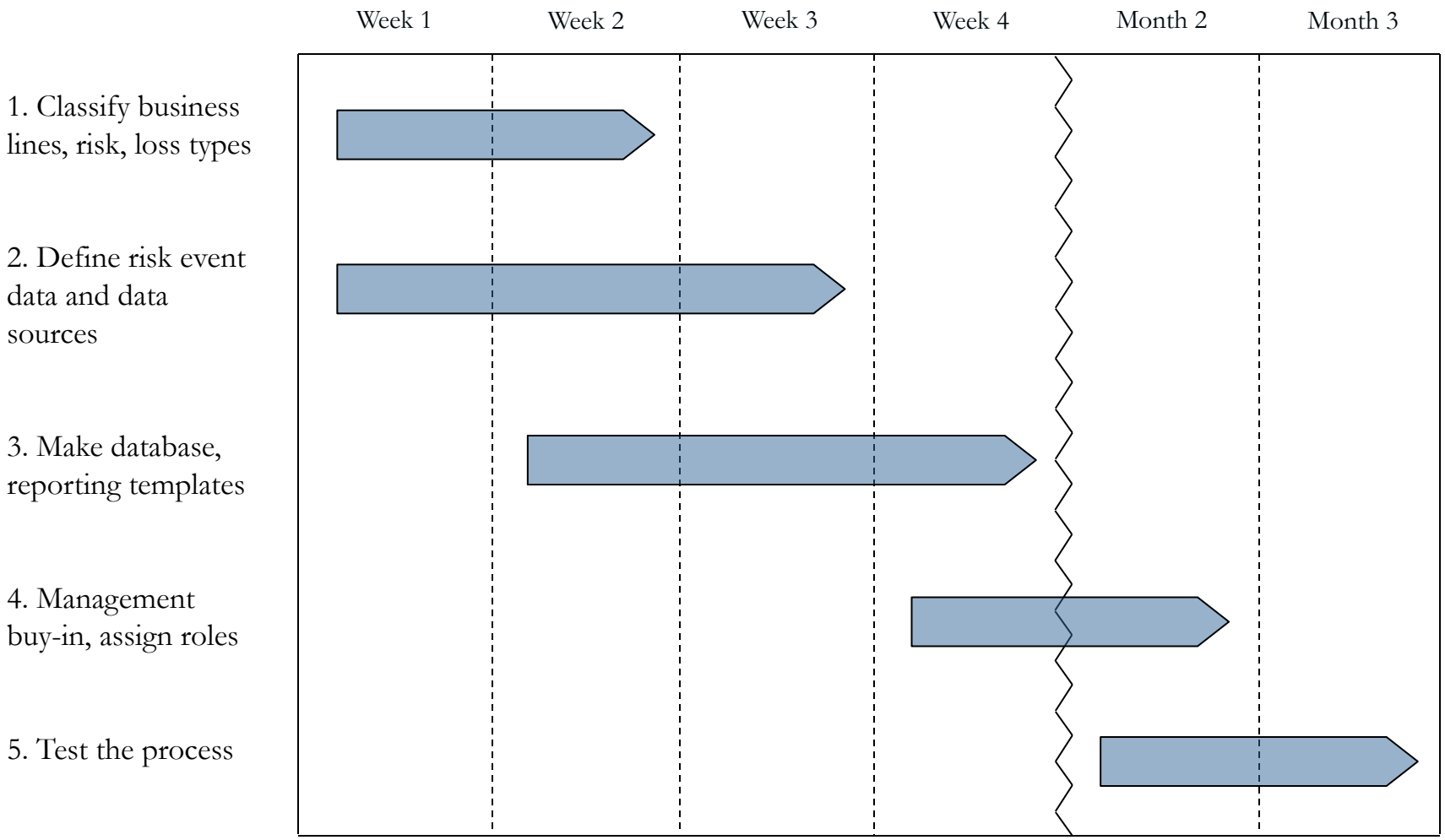


SOURCE: Sungard BancWare

WHY COLLECT DATA?



DATABASE DEVELOPMENT



DATABASE CLASSIFICATORS (1/2)

Business Areas	Risk event types	Loss Types
▪ Corporate Finance ▪ Trading & Sales ▪ **Retail Banking** ▪ **Commercial Banking** ▪ **Payment and Settlement** ▪ Agency Services ▪ Asset Management ▪ Retail Brokerage	▪ Internal fraud ▪ External fraud ▪ Employment Practices and Workplace Safety ▪ Clients, Products & Business Practices ▪ Damage to Physical Assets ▪ Business disruption and system failures ▪ Execution, Delivery & Process Management	**Direct** ▪ Client compensations ▪ Staff payments ▪ Replacement costs ▪ Fees and penalties ▪ Write-offs **Pending Losses** **Provisions** **Indirect** ▪ Timing losses ▪ Opportunity costs ▪ Enhancement costs ▪ Insurance premiums

SOURCES:

1. BASEL II Framework, Annexes 8 and 9

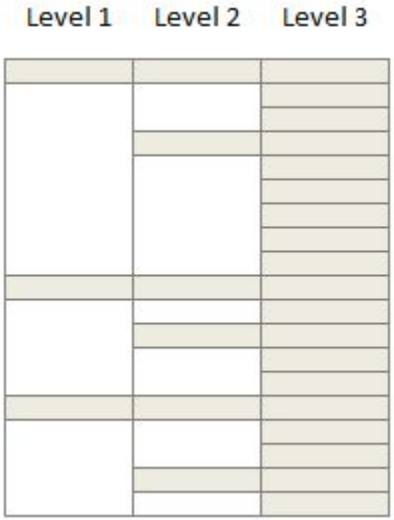
2.Operational Risk – Supervisory Guidelines for the AMA. BCBS, June 2011

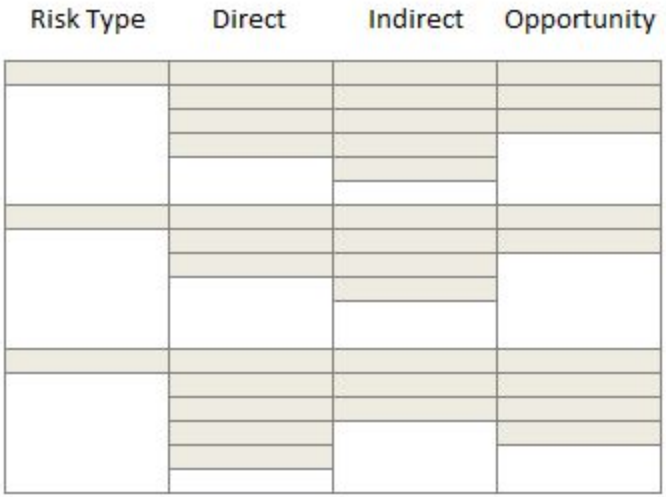
3.Operational risk reporting standards. ORX, Edition 2011. Appendix – Detailed Description of Data Categories

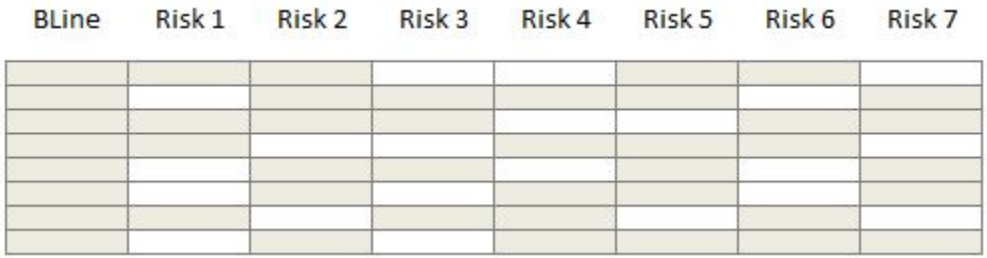
DATABASE CLASSIFICATORS (2/2)

Practical considerations

- ✔ Coding classes (Size and Filtering)
- ✔ Low-level breakdowns of first-rank classes
- ✔ Cross classes matrixes
  - Risk Type – Costs
  - Business Line – Risk Type





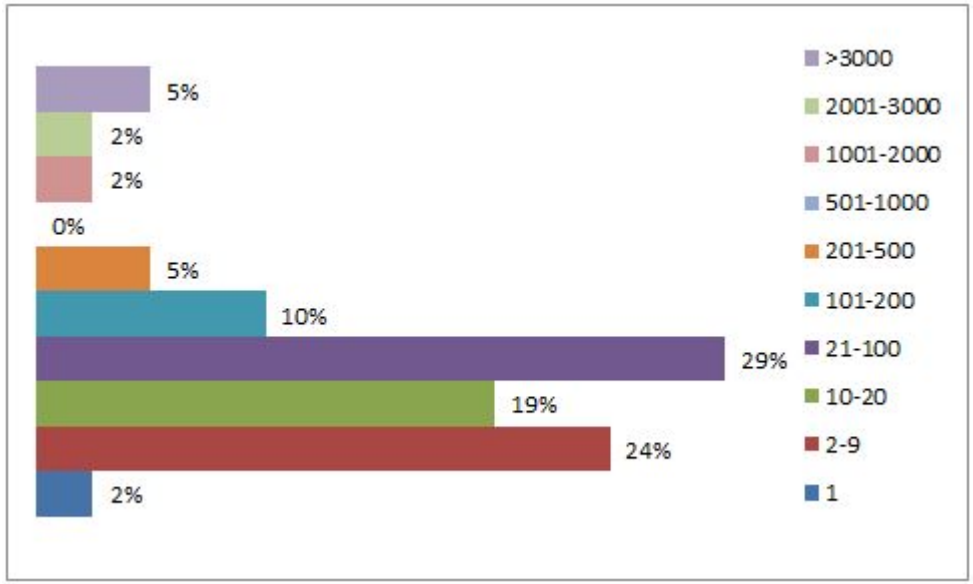


RISK GRANULARITY

BASEL II Framework:

A bank's risk measurement system must be sufficiently 'granular' to capture the major drivers of operational risk affecting the shape of the tail of the loss estimates

- ✔ Medium bank has from 20 to 100 risk categories as listed in Basel II default scheme



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

WHAT DATA ARE ESSENTIAL TO COLLECT?

RECORD DETAILS IDENTIFICATION

- Record date
- Risk owner
- Risk Coordinator
- Date of discovery
- Observer
- Description

ACTIONS

- Actions taken
- Actions to be taken
- Recovery

RISK EVENT DESCRIPTION

- Date of occurring
- Event type
- Risk type
- Risk object
- Description
- Cause

EVALUATION

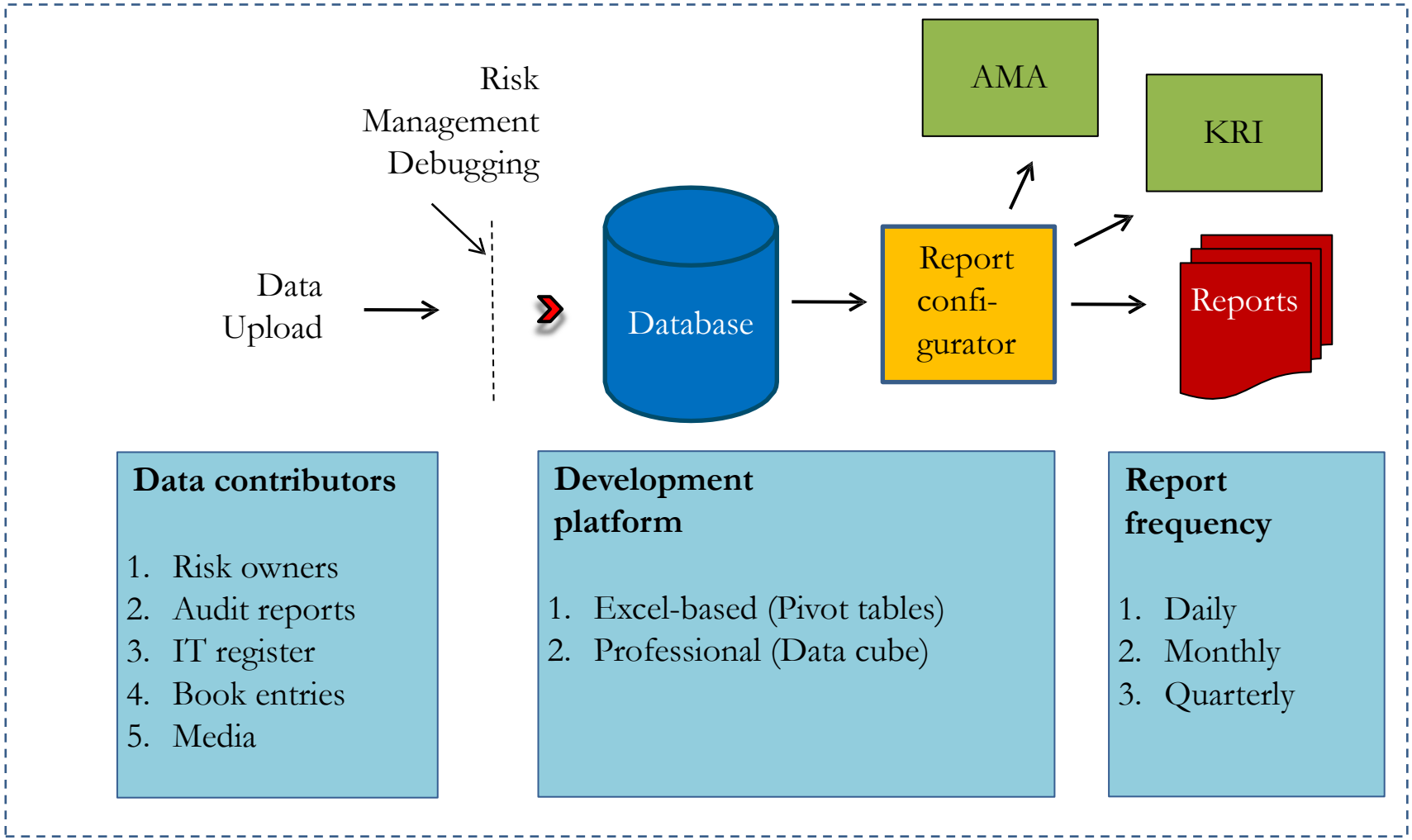
- Direct loss type
- Amount of losses
- Date of accounting
- Indirect losses
- Effect of risk event
- Qualitative Assessment

AUTORIZATION

- Line Manager
- Risk Manager
- Dates of approval
- Corrections
- Data source

NOTE: Key information for risk judgment is highlighted blue

DATABASE FUNCTIONAL MAP



Data contributors

1. Risk owners
2. Audit reports
3. IT register
4. Book entries
5. Media

Development platform

1. Excel-based (Pivot tables)
2. Professional (Data cube)

Report frequency

1. Daily
2. Monthly
3. Quarterly

DATA COLLECTION WORKFLOW

Bank Staff

- Identify risk event
- Inform Coordinator

Real time

Coordinator

- Examine the details of risk event
- Report to Line Manager and Risk Manager
- Fill up the form of risk event record

Real time

Line Manager / Coordinator

- Discuss the details of risk event
- Make suggestions on risk mitigation
- Line Manager reviews and approves the record
- Coordinator submit the record to Risk Manager

Within 24 hours

Risk Manager / Coordinator

- Risk Manager reviews and approves the record
- Risk Manager and Coordinator sort out risk events
- Risk Manager prepares regular reporting

Within 48 hours

Risk Manager / Line Manager

- Agree on consistency of database
- Review findings and make suggestions on risk mitigation

Monthly

DATA COLLECTION: DIFFICULTIES AND SOLUTIONS

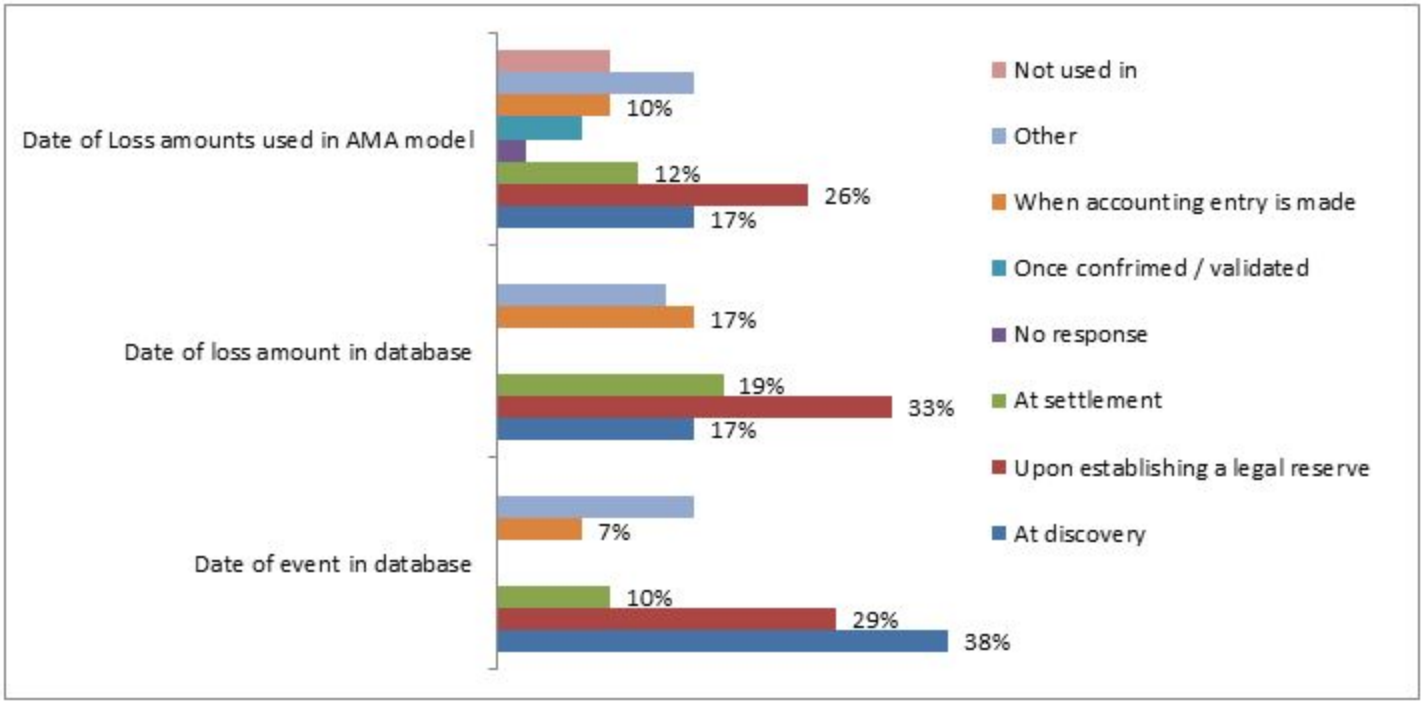
Difficulties

- Lack of knowledge which information to be reported
- Fear of error acknowledgement and punishment
- Feeling solidarity
- No motivation
- Lack of automation

Solutions

- System of risk coordinators, functional subordination
- Formal procedure / Typical risk map
- Higher salary / Bonus / Penalties
- Premiums for rationalization proposals
- Anonymous hot line
- Data verification – KPI, head office registers, B/S accounts
- Automation
- Evaluation / Team building events

KEY DATES OF DATA COLLECTION



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

SPECIFIC EVENT TYPES (1/3)

OpRisk event is an event leading to the actual outcome(s) of a business process to differ from the expected outcome(s), due to inadequate or failed processes, people and systems, or due to external facts or circumstances

- **Single event**
  - Repeated mistakes due to a process failure
  - Multiple impacts from a single cause
  - Fraud losses connected by a common plan of action
  - A technology outage which affects multiple business lines
  - Multiple errors made by a single individual over a period of time

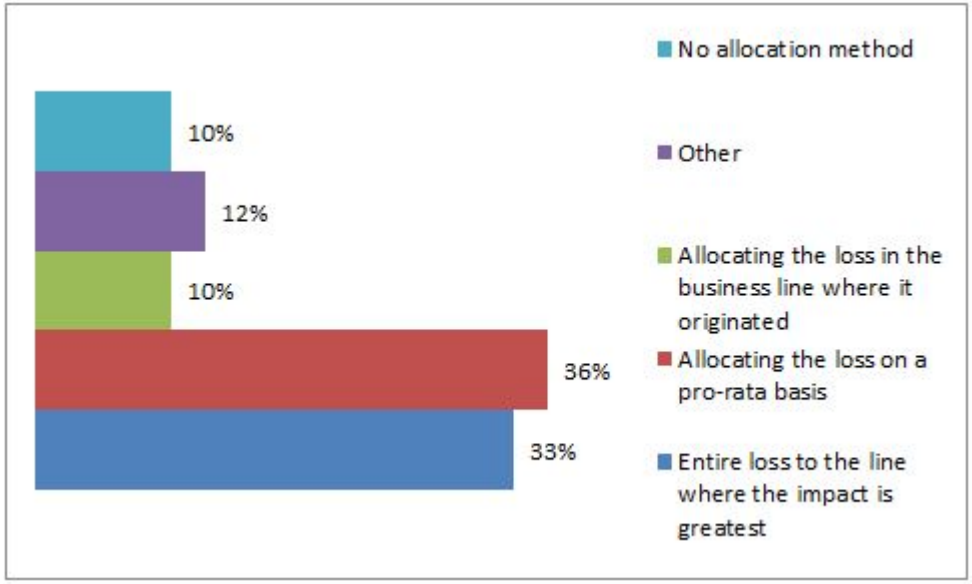
SOURCE: Operational Risk Reporting Standards. ORX, Edition 2011

SPECIFIC EVENT TYPES (2/3)

- **Linked event** – a single event, which impacts more than one business line

Where register losses?

- the owner of the transaction
- business process out of which the event arose
- **the business with the largest P&L impact**
- **to multiple business lines based on P&L split**



SOURCE:

1. Operational Risk Reporting Standards. ORX, Edition 2011

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

SPECIFIC EVENT TYPES (3/3)

- **Near-misses** – operational risk events that did not lead to a loss, but had the potential to do so
  - IT disruptions outside working hours
  - Fault in transmitting erroneous mandatory reports
  - Cancelling doubled printed trading order
  - Grow cold when air condition system is out of operation
- **Operational risk gain events** – operational risk events that generate a gain
  - Trading limit was not observed but position win
  - Product mis-selling that yield profit for the company
  - Making mistake in setting FX rate that brought larger income

SOURCE: Operational Risk – Supervisory Guidelines for the AMA. BCBS, June 2011

SPECIFIC LOSS TYPES (1/2)

OpRisk loss – a negative and quantifiable impact on the P&L due to OpRisk event

- **Single loss** – a total amount of all OpRisk losses pertained to a single loss event

- **Grouped losses** are OpRisk losses with the same underlying cause that arise from single events within a Business Line and between Business Lines.

  For risk calculation and reporting purpose grouped losses have to be considered and recorded as a single ―root event‖

- **Root loss** – the initial single event without which none of the grouped related losses would have occurred

SOURCE: Operational Risk Reporting Standards. ORX, Edition 2011

SPECIFIC LOSS TYPES (2/2)

Example: Disease Outbreak in Hong Kong

	Late Transaction Settlement	External consultants costs	Disinfect building costs	Total	Comment
Trading & Sales	100K	250K	50K	400k	Linked Event
Retail Banking		200k	100k	300k	Linked Event
Asset Mgt		300k	50k	350k	Linked Event
CFinance		100k	5k	105k	Linked Event
Total	100k	850k	205k	1.155k	Grouped loss

Risk event type: Disasters & Public Safety / Natural Disasters & Other Events

Amount of Loss: 1.155k

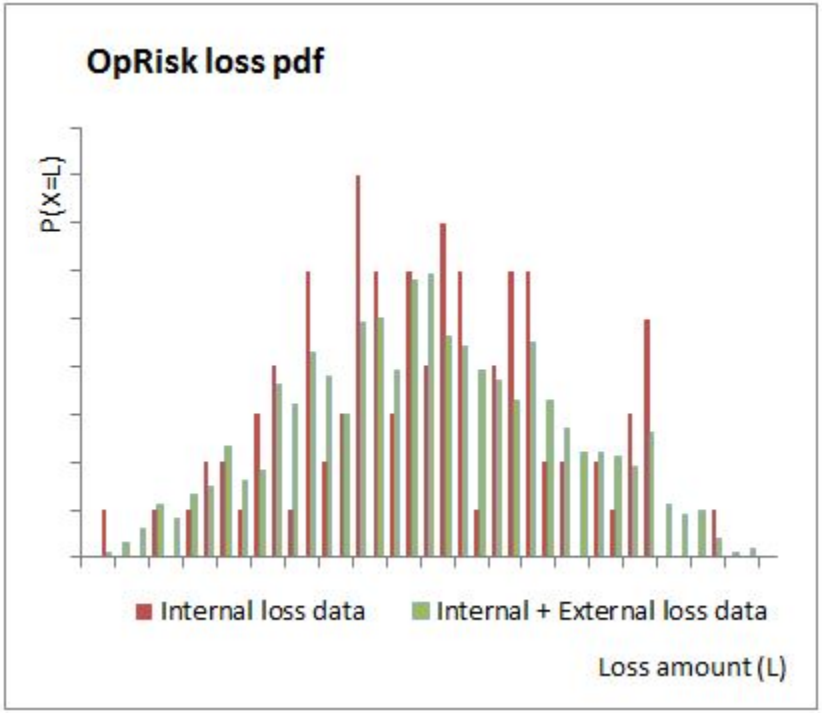
SOURCE: Operational Risk Reporting Standards. ORX, Edition 2011

EXTERNAL LOSS DATA (1/4)

Lack of internal observations → No data integrity and granularity → Low confidence level for measuring risk → Incorrect decision making → Need for external data

Number of observations	Max accuracy	Number of tail observations (1%)
20	95%	-
100	99%	1
1,000	99,9%	10

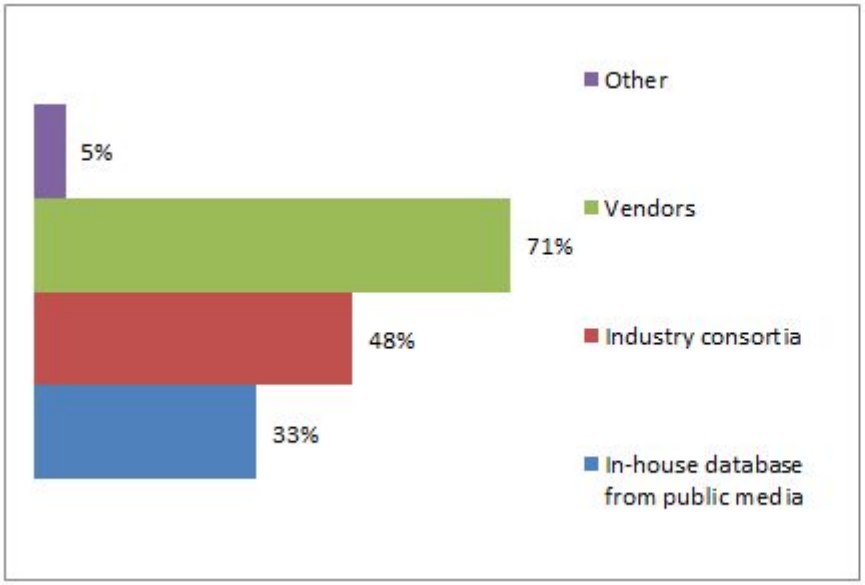
Number of observations	Accuracy	OpVaR
20	95%	124,123
100	95%	159,134
1,000	95%	160,813

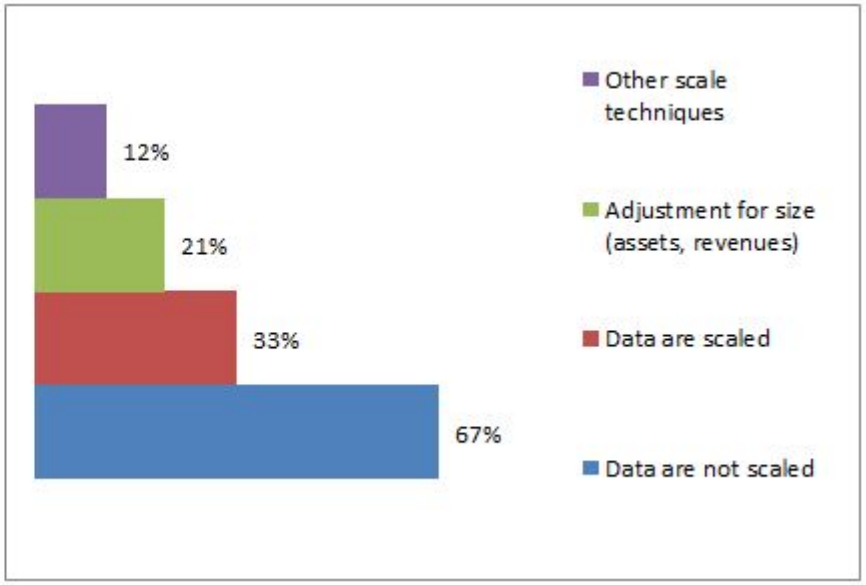


EXTERNAL LOSS DATA (2/4)

External loss data are collected to enlarge sample of high severity events

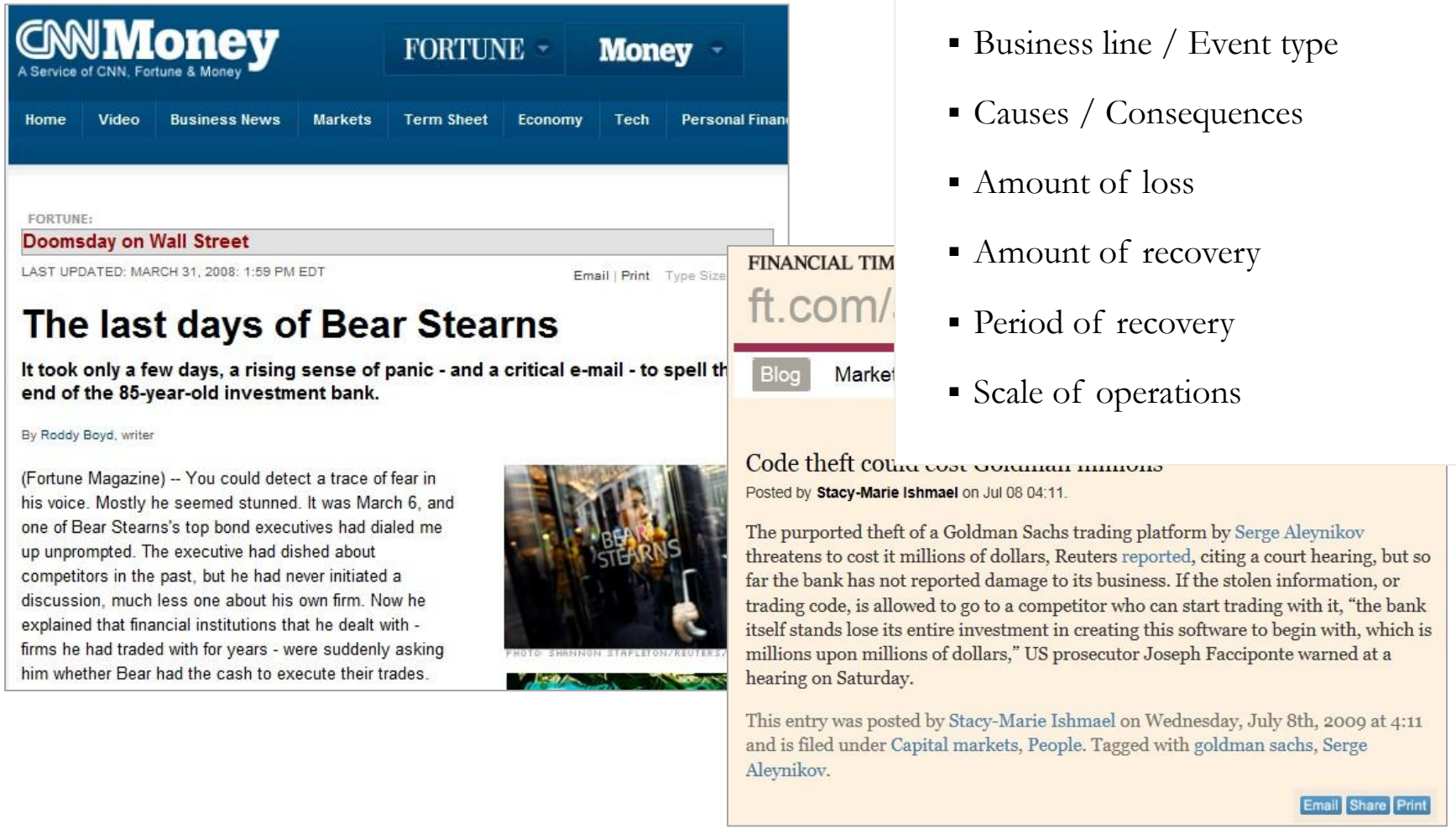
- ✔ Medium international banks rely more on outsourcing rather than own sources
- ✔ Many banks are scaling external data for their parameters





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

EXTERNAL LOSS DATA (3/4)



Key information

- Business line / Event type
- Causes / Consequences
- Amount of loss
- Amount of recovery
- Period of recovery
- Scale of operations

QUIZ: EXTERNAL LOSS DATA – local examples

Internal fraud

External fraud ☐

☐

Reputational risk

☐

Products and processes

☐

☐

System failures and disruptions

☐

External events

☐

☐

RISK EVENT DATA REPORTING MATRIX

Reporting Area	Reporting time	Risk Owner	Risk Man	Audit	OR Com	MB
Typical loss risk event	•Immediate	R	C	-	-	-
Large loss risk event	•Immediate	R	C/R	I	I	I
Risk events observed	•Daily	R	C/R	-	I	-
Register check	•Monthly	C/A	R	I	-	-
Register report	•Monthly	I	R	I	I	-
Summary report	•Quarterly	I	R	I	I	I

KEY RISK REPORTS: 8x7 Matrix

Report shows distribution of frequency, severity and loss amount by business/risk types

Sum and Distribution of Annualised Loss Frequencies by Business Line and Event Type

	Internal Fraud	External Fraud	Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption & System Failures	Execution, Delivery & Process Management	All	Business Line Losses as Percent of All Losses
Corporate Finance	3.5	11.5	21.6	100.2	2.4	4.6	69.1	212.9	0.7%
	1.7%	5.4%	10.2%	47.0%	1.1%	2.2%	32.5%		
Trading & Sales	32.2	31.7	96.9	398.6	12.2	157.6	2,400.6	3,129.9	9.6%
	1.0%	1.0%	3.1%	12.7%	0.4%	5.0%	76.7%		
Retail Banking	979.4	7,311.9	3,203.4	2,381.0	245.4	293.8	3,743.4	18,158.3	55.8%
	5.4%	40.3%	17.6%	13.1%	1.4%	1.6%	20.6%		
Commercial Banking	69.6	710.4	104.3	504.4	30.1	65.2	1,196.8	2,680.8	8.2%
	2.6%	26.5%	3.9%	18.8%	1.1%	2.4%	44.6%		
Payment & Settlement	20.5	185.3	23.3	50.7	21.7	37.5	386.0	725.1	2.2%
	2.8%	25.6%	3.2%	7.0%	3.0%	5.2%	53.2%		
Agency Services	11.3	94.5	12.8	44.9	5.9	26.8	698.9	895.0	2.7%
	1.3%	10.6%	1.4%	5.0%	0.7%	3.0%	78.1%		
Asset Management	10.7	19.1	30.3	96.5	1.9	22.9	522.8	704.2	2.2%
	1.5%	2.7%	4.3%	13.7%	0.3%	3.2%	74.2%		
Retail Brokerage	196.5	75.9	149.4	2,247.0	2.4	16.1	672.7	3,359.9	10.3%
	5.8%	2.3%	4.4%	66.9%	0.1%	0.5%	20.0%		
Unallocated	50.5	124.7	2,072.4	91.6	61.0	17.8	280.1	2,698.2	8.3%
	1.9%	4.6%	76.8%	3.4%	2.3%	0.7%	10.4%		
All	1,374.3	8,564.9	5,714.5	5,914.9	382.9	642.3	9,970.5	32,564.3	100.0%
	4.2%	26.3%	17.5%	18.2%	1.2%	2.0%	30.6%		

SOURCE: Results from the 2008 Loss Data Collection Exercise for Operational Risk. BCBS, July 2009

KEY RISK REPORTS: 8x7 Matrix

Report shows distribution of frequency, severity and loss amount by business/risk types

Sum and Distribution of Annualised Loss Amounts (€Millions) by Business Line and Event Type

	Internal Fraud	External Fraud	Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption & System Failures	Execution, Delivery & Process Management	All	Business Line Loss Amount as Percent of Total
Corporate Finance	6.6	3.2	16.2	2,565.1	0.1	0.6	146.7	2,738.5	28.0%
	0.2%	0.1%	0.6%	93.7%	0.0%	0.0%	5.4%		
Trading & Sales	145.8	4.5	30.3	384.7	2.7	23.8	732.6	1,324.4	13.6%
	11.0%	0.3%	2.3%	29.0%	0.2%	1.8%	55.3%		
Retail Banking	198.5	607.9	305.6	1,263.6	34.0	48.0	670.6	3,128.0	32.0%
	6.3%	19.4%	9.8%	40.4%	1.1%	1.5%	21.4%		
Commercial Banking	84.7	112.8	23.1	262.4	3.3	12.7	241.2	740.2	7.6%
	11.4%	15.2%	3.1%	35.5%	0.4%	1.7%	32.6%		
Payment & Settlement	7.1	18.1	2.3	18.7	8.0	5.8	194.4	254.4	2.6%
	2.8%	7.1%	0.9%	7.3%	3.2%	2.3%	76.4%		
Agency Services	2.5	8.1	1.7	92.3	46.7	15.4	89.8	256.5	2.6%
	1.0%	3.2%	0.7%	36.0%	18.2%	6.0%	35.0%		
Asset Management	27.0	2.3	6.1	74.9	0.6	3.6	128.3	242.9	2.5%
	11.1%	1.0%	2.5%	30.8%	0.3%	1.5%	52.8%		
Retail Brokerage	89.8	6.7	31.1	294.6	0.4	1.0	71.5	495.1	5.1%
	18.1%	1.4%	6.3%	59.5%	0.1%	0.2%	14.4%		
Unallocated	38.5	16.3	167.1	166.8	38.3	7.6	154.0	588.5	6.0%
	6.5%	2.8%	28.4%	28.3%	6.5%	1.3%	26.2%		
All	600.5	780.0	583.4	5,123.1	134.0	118.4	2,429.2	9,768.5	100.0%
	6.1%	8.0%	6.0%	52.4%	1.4%	1.2%	24.9%		

SOURCE: Results from the 2008 Loss Data Collection Exercise for Operational Risk. BCBS, July 2009

KEY RISK REPORTS: Severity Distribution

Report shows distribution of frequency and loss amount by loss severity brackets

Loss severity (X)	Number of Losses	Number of Losses, % Total	Loss Severities, € thousands	Loss Severity, % of Largest	Amount of Losses, € mln	Amount of Losses, % of Total	Amount of Losses Net of Recoveries	Amount of Losses Net of Recoveries, % of Total
€0 ≤ X < €20,000	9 897 083	98,5%	1,2	0,0%	12 164	18,9%	3 090	16,7%
€20,000 ≤ X < €100,000	121 533	1,2%	42,6	0,0%	5 178	8,1%	1 528	8,3%
€100,000 ≤ X < €1 Million	30 598	0,3%	264,2	0,0%	8 085	12,6%	2 385	12,9%
€1 Million ≤ X < €2 Million	1 688	0,0%	1 422,4	0,3%	2 401	3,7%	708	3,8%
€2 Million ≤ X < €5 Million	1 116	0,0%	3 198,9	0,6%	3 570	5,6%	1 053	5,7%
€5 Million ≤ X < €10 Million	404	0,0%	6 997,5	1,3%	2 827	4,4%	834	4,5%
€10 Million ≤ X < €100 Million	333	0,0%	24 753,8	4,7%	8 243	12,8%	2 432	13,2%
€100 Million ≤ X	41	0,0%	530 536,6	100,0%	21 752	33,9%	6 417	34,8%
TOTAL	10 052 796	100,0%	6,4	0,0%	64 220	100,0%	18 446	100,0%

KEY RISK REPORTS: Summary Report

Report aggregates frequency and loss amount by business / risk types

Business Line	Number of Losses	Number of Losses, % Total	Amount of Losses, €	Amount of Losses, % of Total	Number of Losses ≥ €20,000	Number of Losses ≥ €20,000, % of Total	Amount of Losses ≥ €20,000	Amount of Losses, % of Total ≥ €20,000
Corporate Finance	18	0,9%	1 453 304	6,1%	6	4,0%	1 395 680	6,9%
Trading & Sales	127	6,4%	3 786 142	15,8%	16	11,0%	3 368 852	16,7%
Retail Banking	550	27,7%	4 478 410	18,7%	32	21,2%	3 527 350	17,5%
Commercial Banking	80	4,0%	1 535 393	6,4%	10	6,6%	1 434 272	7,1%
Payment and Settlement	415	20,9%	723 872	3,0%	10	6,5%	677 171	3,4%
Agency Services	278	14,0%	3 571 847	14,9%	28	18,9%	2 897 325	14,4%
Asset Management	69	3,5%	2 480 506	10,3%	14	9,2%	2 252 126	11,2%
Retail Brokerage	450	22,6%	5 967 705	24,9%	34	22,6%	4 616 148	22,9%
TOTAL	1 987	100,0%	23 997 179	100,0%	149	100,0%	20 168 923	100,0%

KEY RISK REPORTS: Register Report

Report lists key parameters of risk events collected in database during reporting period

OPRISK EVENT REGISTER REPORT

#	Risk Event ID	Date of Risk Event	Risk Owner	Risk type	Risk Object	Causes of risk event	Effects of risk event	Actions taken	Near Misses (Y/N)	Number of events	Losses net of Recoveries	Priority
Business Unit 1										**1**	**500**	**M**
1	111-2803-1	28.03	BU1	Regulatory breach	Mandatory ratios	Lack of control	Penalties	Strengthen control	N	1	500	M
Business Unit 4										**5**	**250 000**	**H**
2	811-1403-1	14.03	BU4	Pricing error	FX rates	Negligence	Not identified	Official reprimand	Y	1	-	L
3	811-2103-1	21.03	BU4	Loss of loan documentation	Commercial Loan	Unknown	Non-performing loans	Internal investigation	N	4	250 000	H
Business Unit 7										**18**	**6 000**	**M**
4	212-1503-1	15.03	BU7	Processing error	Client accounts	No automatic control	Client compensation	Automatic controls	N	16	1 000	M
5	212-1903-1	19.03	BU7	Data error	Money transfer	Disregard	Client compensation	Dismissal	N	2	5 000	M
Branch 1										**1**	**-**	**M**
6	311-1703-1	17.03	Branch 1	IT system failure	IT system	Internal error	4 hours downtime	System patch	Y	1	-	M
Branch 3										**3**	**10 000**	**H**
7	503-1003-1	10.03	Branch 3	Misseling	Utility payments	Lack of experience	Opportunity costs	Additional training	Y	2	-	L
8	503-2403-1	24.03	Branch 3	Compromising	Customer information	Disregard	Client compensation	Official apologise	N	1	10 000	H
Branch 7										**35**	**130 000**	**H**
9	923-1403-2	14.03	Branch 7	External fraud	Credit cards	Faulty business process	Theft	Police investigation	N	34	130 000	H
10	923-1103-1	11.03	Branch 7	IT disruption	Internet connection	External event	2 hours downtime	Provider change	Y	1	-	M

MANAGEMENT BUY-IN

DATABASE SET INCLUDES:

- Classifications matrixes
- Data structure
- Reporting templates

- Workflow guidelines
- Job descriptions of key involved parties

- Testing group / Action plan

REVIEW: Operational Risk Committee

APPROVAL: Management Board

Table of Contents

Pillar II. Risk Measurement and Analysis

1. Risk event data collection
2. Capital Requirement
3. Scenario analysis

SOUND PRACTICE

Basel Committee on Banking Supervision
Principles for the Sound Management of Operational Risk, June 2011

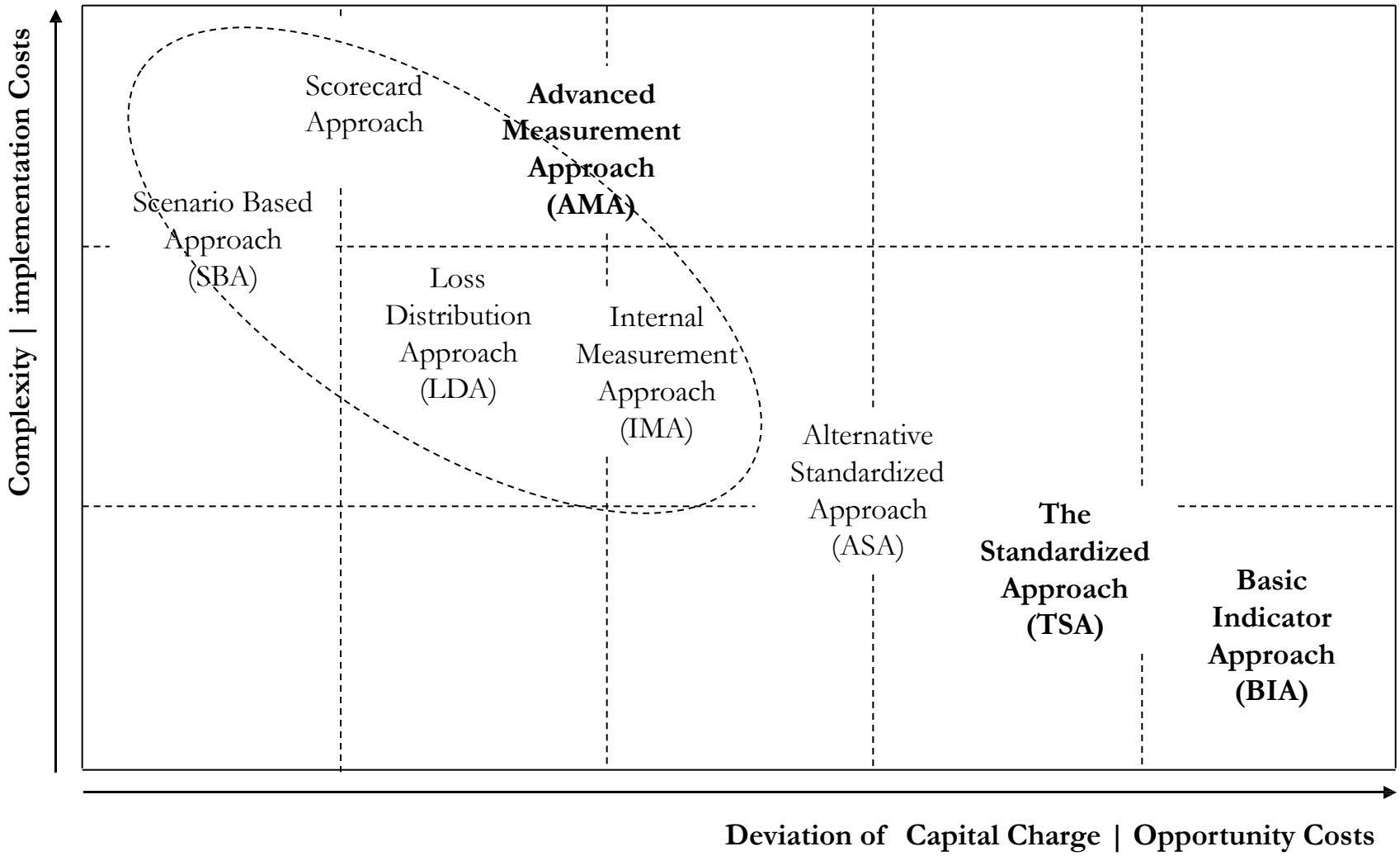
— Measurement: Larger banks may **find it useful to quantify their exposure to operational risk** by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return‖

Basel II Framework

Calculation of minimum capital requirements

$$CAR = \frac{Equity}{RWA + 12.5 \times MRisk + 12.5 \times OpRisk} \geq 0.08$$

MEASUREMENT APPROACHES



SELECTION CRITERIA

- Complexity or intensity of banking operations
- Meeting qualitative standards
- Partial use
- Restriction to revert to a simpler approach

BASIC INDICATOR APPROACH (1/2)

The simplest approach based on linear dependence between income as key exposure indicator and capital charge behind OpRisk

$$L_{BIA} = \left[\sum \left(GI_{1,\ldots,n} \times \alpha\right)\right] / n \quad \mid \quad GI_{1,\ldots,n} > 0,\ n \in [0;3],\ \alpha = 0{,}15$$

Advantages: ▪ Simplicity

Shortcomings:
- Linear relationship with exposure indicator
- Non-specific to business type
- Exposure indicator is distorted with business cycle (lower in downturn, higher in upturn)

BASIC INDICATOR APPROACH (2/2)

Indicator	Year 1	Year 2	Year 3
Net Interest Income	**(100)**	**15**	**20**
Interest Income	100	150	250
Interest Expenses	(200)	(135)	(230)
Net Non-interest Income	**35**	**13**	**17**
Non-interest Income	45	48	29
Non-interest Expenses	(10)	(35)	(12)
Additions (not excluded)	**5**	**7**	**8**
Provisions (for unpaid income)	4	5	7
Operating expenses (outsourcing fees paid)	1	2	1
Deductions (to be excluded)	**(5)**	**(3)**	**(2)**
Realized P&L on securities in BB	(5)	(3)	(1)
Extraordinary items	0	0	(1)
Gross Income	**(70)**	**25**	**35**
Capital Charge with BIA	**$(25+35)/2 \cdot 0.15 = 4.5$**		

THE STANDARDIZED APPROACH (1/3)

More accurate approach sensitive to business line segmentation

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

Advantages:

- Fairly simple
- Specific to business type

Shortcomings:

- Linear relationship with risk driver
- Exposure indicator is distorted with business cycle (lower in downturn, higher in upturn)

THE STANDARDIZED APPROACH (2/3)

	Indicator	Corporate finance	Trading and Sales	Retail Banking	Commercial Banking	Payment and Settlement	Agency Services	Asset Management	Retail Brokerage	Total
Year 1	Gross Income	0	(20)	200	(270)	15	2	3	0	(70)
	Beta	18%	18%	12%	15%	18%	15%	12%	12%	-
	Capital Charge	**0**	**(3.6)**	**24**	**(40.5)**	**2.7**	**0.3**	**0.36**	**0**	**< 0**
Year 2	Gross Income	5	15	80	(-90)	12	1	2	0	25
	Beta	18%	18%	12%	15%	18%	15%	12%	12%	-
	Capital Charge	**0.9**	**2.7**	**9.6**	**(13.5)**	**2.16**	**0.15**	**0.24**	**0**	**2.25**
Year 3	Gross Income	2	(5)	20	10	5	2	1	0	35
	Beta	18%	18%	12%	15%	18%	15%	12%	12%	-
	Capital Charge	**0.36**	**(0.96)**	**2.4**	**1.5**	**0.96**	**0.3**	**0.12**	**0**	**4.68**
	Capital Charge with TSA	**(2.25+4.68)/3 = 2.31 < 4.5 (BIA)**								

THE STANDARDIZED APPROACH (3/3)

Minimum qualifying criteria for TSA:

- Management oversight of ORM framework
- Soundness and integrity of ORM system
- Sufficient resources in ORM across major business lines, control and audit
- Specific policies developed and criteria documented for mapping gross income for current business lines and activities

ALTERNATIVE STANDARDIZED APPROACH (1/3)

A modification to TSA encompassing volume exposure indicator

$$\begin{cases} K_{ASA} = \left\{ \sum_{\text{years 1-3}} \max \left[\sum \left(K_{GI} + K_{LA} \right), 0 \right] \right\} / 3, \\ K_{GI} = \sum \left(GI_i \times \beta_i \right), \ i = 1, 2, 5, \ldots, 8, \\ K_{LA} = \sum \left(\beta_i \times m \times LA_i \right), \ i = 3, 4 \end{cases}$$

Advantages:

- Fairly simple
- Specific to business type
- More stable prediction through business cycle

Shortcomings:

- Linear relationship with exposure indicators

ALTERNATIVE STANDARDIZED APPROACH (2/3)

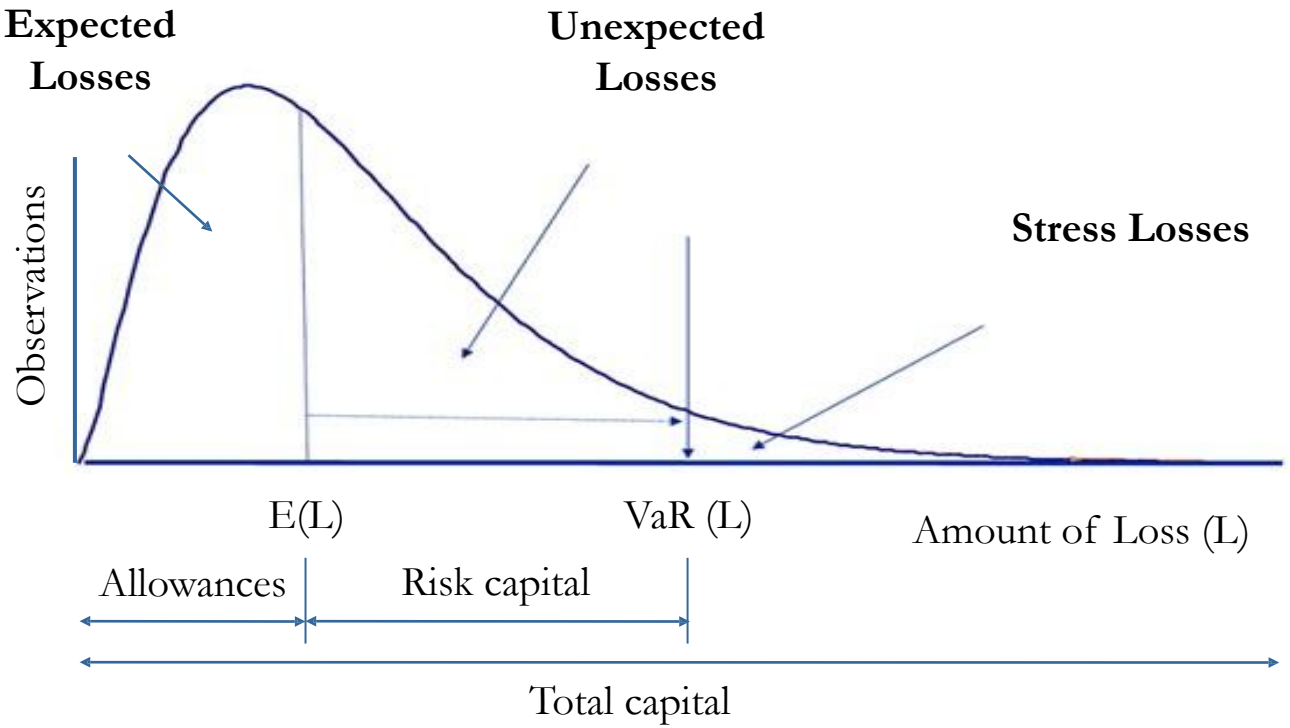
	Indicator	Year 1	Year 2	Year 3	Average
Retail loans	**Outstanding loans**	**2,200**	**2,500**	**2,850**	**2,517**
	Retail loans	2,000	2,500	2,750	2,417
	SME loans treated as retail	500	400	650	517
	Purchased receivables	50	100	150	100
	Provisions	(350)	(500)	(700)	(517)
	Exposure indicator	**(0.035 · 2,517) = 88**			
Corporate loans	**Outstanding loans**	**4,150**	**5,375**	**6,050**	**5,192**
	Corporate loans	3,000	3,500	3,750	3,417
	Sovereign / Bank / Specialized lending	500	750	1,000	750
	Securities held in BB	250	300	350	300
	SME loans treated as corporate	1,000	1,400	1,650	1,350
	Purchased receivables	250	375	400	342
	Provisions	(850)	(950)	(1,100)	(967)
	Exposure indicator	**(0.035 · 5,192) = 182**			

ALTERNATIVE STANDARDIZED APPROACH (3/3)

	Indicator	Corporate finance	Trading and Sales	Retail Banking	Commercial Banking	Payment and Settlement	Agency Services	Asset Management	Retail Brokerage	Total
Year 1	Exposure Indicator	0	(20)	88	182	15	2	3	0	-
	Beta	18%	18%	12%	15%	18%	15%	12%	12%	-
	Capital Charge	**0**	**(3.6)**	**10.56**	**27.3**	**2.7**	**0.3**	**0.36**	**0**	**37.62**
Year 2	Exposure Indicator	5	15	88	182	12	1	2	0	-
	Beta	18%	18%	12%	15%	18%	15%	12%	12%	-
	Capital Charge	**0.9**	**2.7**	**10.56**	**27.3**	**2.16**	**0.15**	**0.24**	**0**	**44.01**
Year 3	Exposure Indicator	2	(5)	88	182	5	2	1	0	-
	Beta	18%	18%	12%	15%	18%	15%	12%	12%	-
	Capital Charge	**0.36**	**(0.96)**	**10.56**	**27.3**	**0.96**	**0.3**	**0.12**	**0**	**38.64**
	Capital Charge with TSA	**(37.62+44.01+38.64)/3 = 40.09 >> 4.5 (BIA) > 2.31 (TSA)**								

ADVANCED MEASUREMENT APPROACHES (1/3)

Capital Charge with AMA = Expected Losses (EL) + Unexpected Losses (UL)



ADVANCED MEASUREMENT APPROACHES (2/3)

Qualifying standards:

- Meeting minimum qualifying criteria used for TSA
- Having independent full-fledged ORM function
- ORM is closely integrated in day-to-day activity
- Regular reporting and action taking processes
- ORM practice is documented, reviewed / validated internally and externally

ADVANCED MEASUREMENT APPROACHES (3/3)

Quantitative standards:

- Capture potentially severe _tail' loss events at one year holding period and a 99.9th percentile confidence interval
- Risk model and its validations should be based on data history not less than 3 years (at initial recognition) and over 5 years (in next calculations)
- Be consistent with scope of BCBS OpRisk definition and loss event types
- Capital charge should cover EL and UL, if EL is not provisioned properly
- Should be sufficiently _granular' to capture the major drivers of OpRisk affecting the shape of the tail of the loss estimates
- Correlations across individual operational risk estimates should be recognized by the regulators as sound and implemented with integrity
- Must include the use of internal data, relevant external data, scenario analysis, RCSA and KRI/KPI with credible, transparent, well-documented and verifiable approach for weighting the elements in overall ORM system

INTERNAL MEASUREMENT APPROACH (1/2)

Approach based on linear proxy between expected and unexpected losses

$$L_{IMA} = \sum \left(\gamma_{ij} \times EL_{ij} \right)$$

$$EL_{ij} = EI_{ij} \times PE_{ij} \times LGE_{ij}$$

$$PE_{ij} = \frac{\sum EI_{ij} \mid_{LE_{ij}>0}}{\sum EI_{ij}}$$

$$LGE_{ij} = \frac{\sum LE_{ij}}{\sum NE_{ij}}$$

Parameters

γ – proxy parameter between EL and UL

PE – probability of loss event during 1 year horizon

LGE – average loss given that an event occurs

EI – exposure indicator to capture the scale of activities for business line i/event type j

LE – single loss event

NE – number of single loss events

Exposure indicators

- Number of transactions
- Average volume of transactions
- Total turnover of operations
- Gross income of operations

SOURCES: 1. Working Paper on the Regulatory Treatment of Operational Risk BCBS, 2001
2. Carol Alexander. Operational Risk: Regulation, Analysis and Management, Pearson Education, 2003, p.148

INTERNAL MEASUREMENT APPROACH (2/2)

Advantages

- Flexibility of exposure indicators
- Specific to business type
- Dependent on internal losses

Shortcomings

- Linear proxy between EL and UL

Indicator	EI	PE	LGD	EL	γ	Charge
Corporate finance	20	0.2%	20	0.8	7.8	6.2
Trading and Sales	1,000	1%	0.1	1	3.4	3.4
Retail Banking	5,000	5%	0.01	2.5	4.2	10.5
Commercial Banking	750	0.1%	5	3.75	5.4	20.3
Payment and Settlement	50,000	0.005%	1.5	3.75	6.6	24.7
Agency Services	15	0.1%	50	0.75	4.5	3.4
Asset Management	4	0.3%	40	0.48	5.7	2.7
Retail Brokerage	25	0.1%	25	0.625	3.8	2.4
Capital charge with IMA						**73.7**

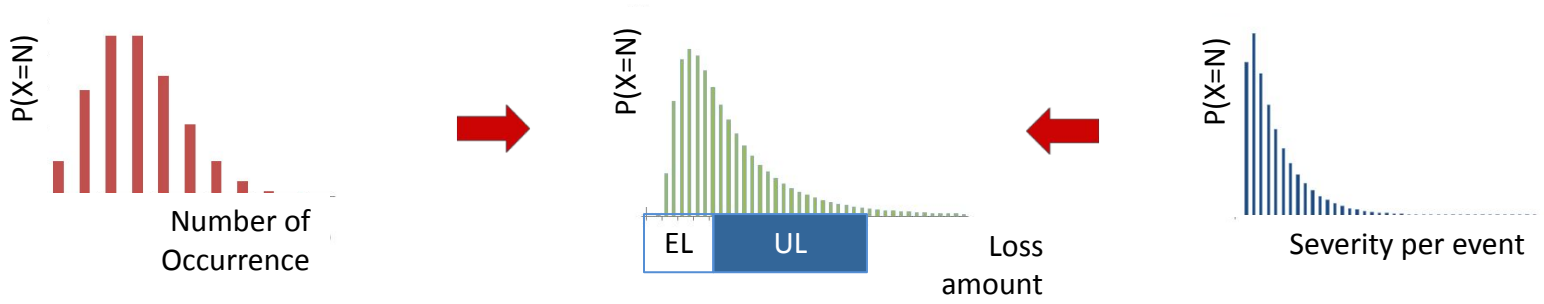
LOSS DISTRIBUTION APPROACH (1/6)

LDA estimates for each business line / event type the likely distribution of OpRisk losses over certain period of time (1 year) at required confidence level (99,9%)

LDA measures UL directly with the loss distribution derived from assumptions of loss frequency and severity distributions an correlations between loss events

$$L_{AMA} = \sum \left[OpRisk_{ij}(1Y@99.9\%) - EL_{ij} \right] - \rho$$

Frequency distribution **Loss distribution** **Severity distribution**



LOSS DISTRIBUTION APPROACH (2/6)

OpRisk Loss Simulation Algorithm:

1. Collect statistics on loss events no. per day and severity per event within 3 years period
2. Select theoretical distributions and derive their parameters from the sample
3. Construct empirical and theoretical distributions – pmfs, pdfs and cdfs
4. Make goodness-of-fit tests and select distributions passed the test
5. Simulate a vector of frequency and matrix of severities with selected distributions
6. Sum severities for simulated frequency and obtain daily loss
7. Repeat steps 5 and 6 at least 10.000 times and get a vector of daily losses
8. Compute annual losses with a sliding scale of 250 days
9. Take 99.9% percentile from the sample of annual losses obtained (OpVaR)
10. Compute the mean of simulated annual losses (EL)

OpRisk for single business line and event type = OpVaR – EL

(if EL is adequately provisioned)

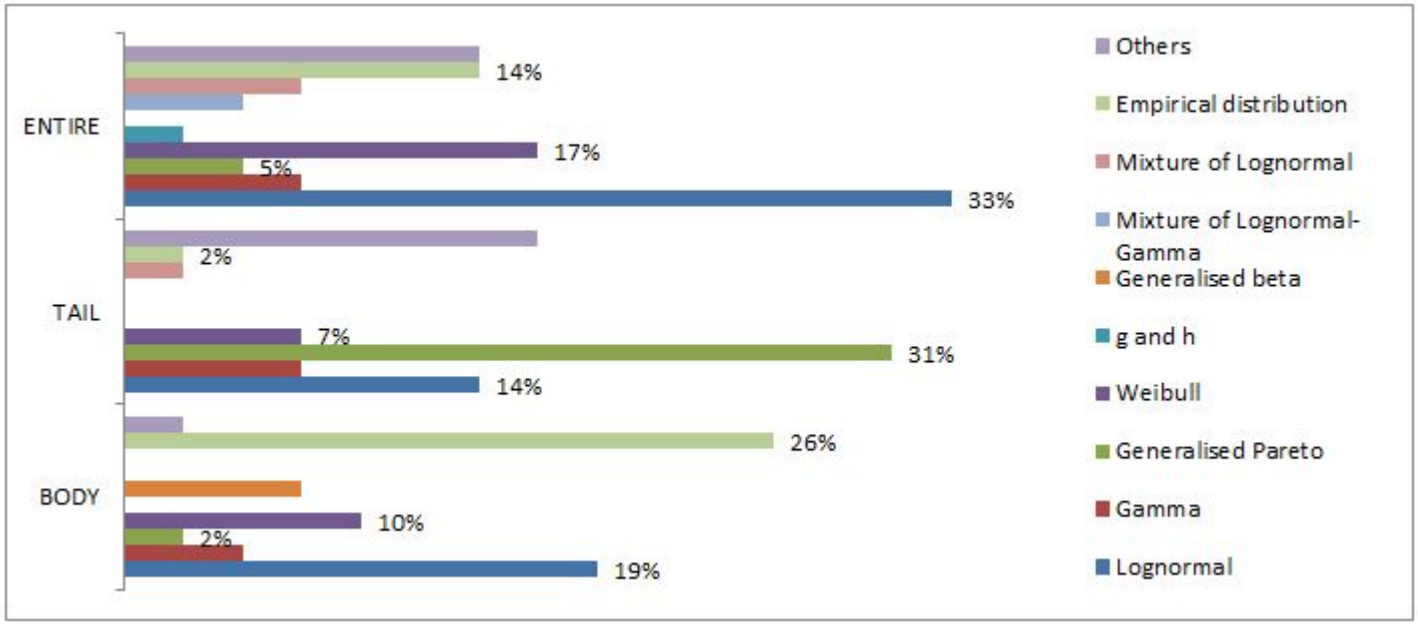
LOSS DISTRIBUTION APPROACH (3/6)

Severity distributions

- Lognormal
- Pareto
- Weibull

Validation tests

- Q-Q plot
- K-S test



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

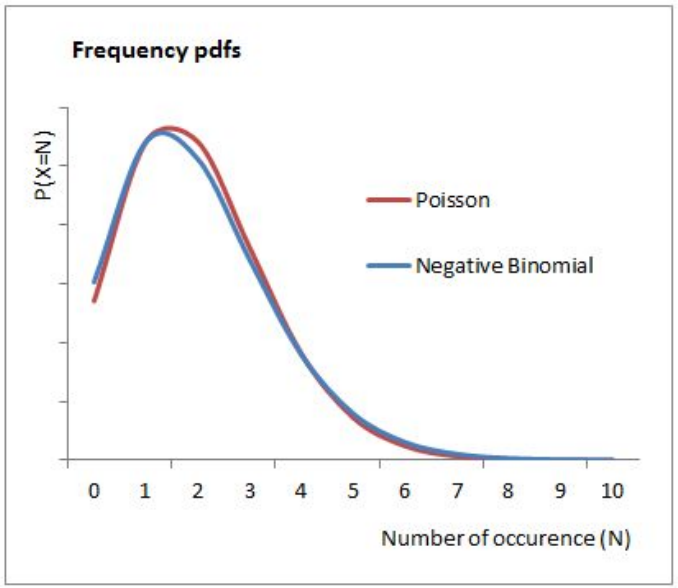
LOSS DISTRIBUTION APPROACH (4/6)

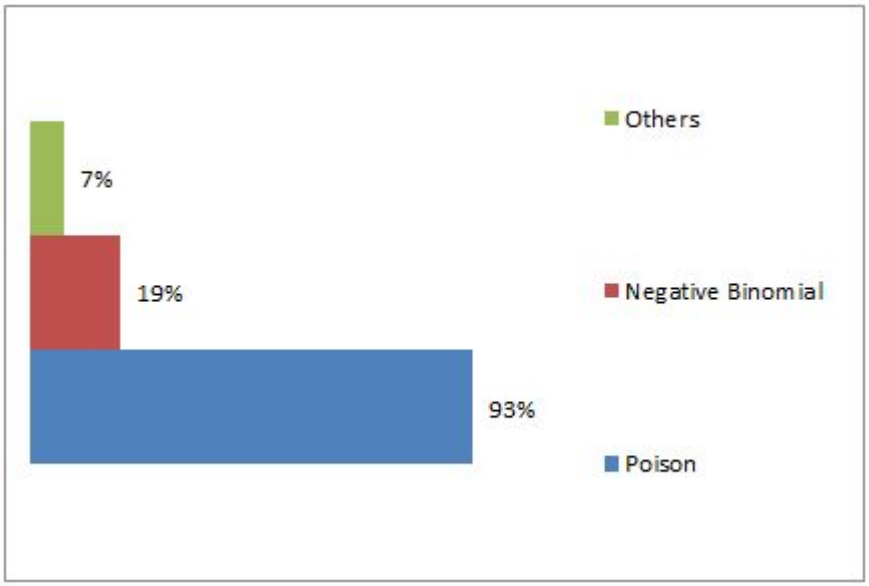
Frequency distributions

- Poisson
- Negative Binomial

Validation tests

- χ^2-test

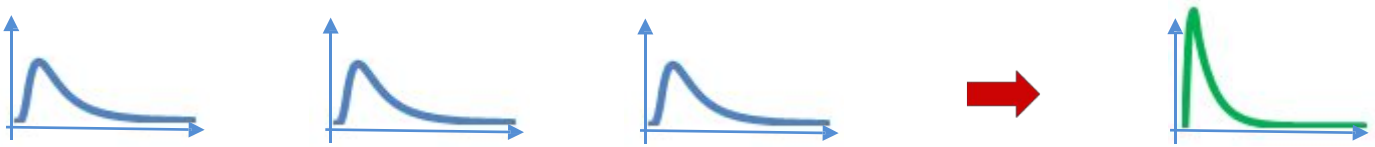




SOURCE: Observed range of practice in key elements of Advanced Measurement Approaches (AMA). BCBS, July 2009

LOSS DISTRIBUTION APPROACH (5/6)

Loss aggregation



BU/ET 1 | BU/ET … | BU/ET n | Gross Loss

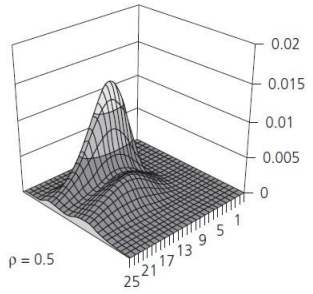
- No diversification: $\sum \left[OpRisk_{ij}(1Y@99.9\%) - EL_{ij} \right]$
- Fully diversified: $\left(\sum \left[OpRisk_{ij}(1Y@99.9\%) - EL_{ij} \right]^2 \right)^{1/2}$
- Dependency structure based on multivariate distribution functions (copulas)

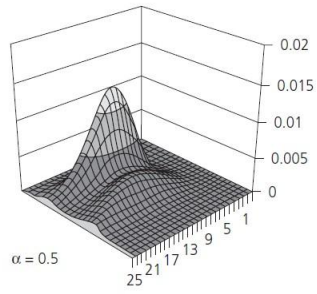
SOURCE: Carol Alexander. Operational Risk: Regulation, Analysis and Management, Pearson Education, 2003

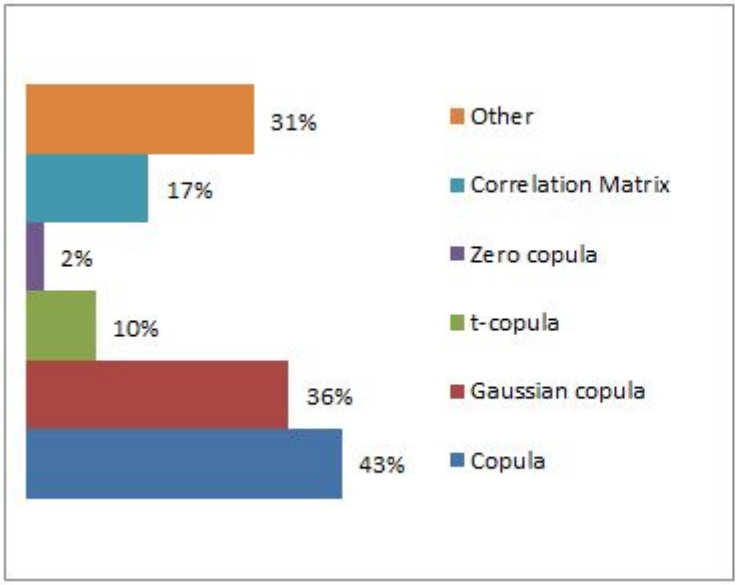
LOSS DISTRIBUTION APPROACH (6/6)

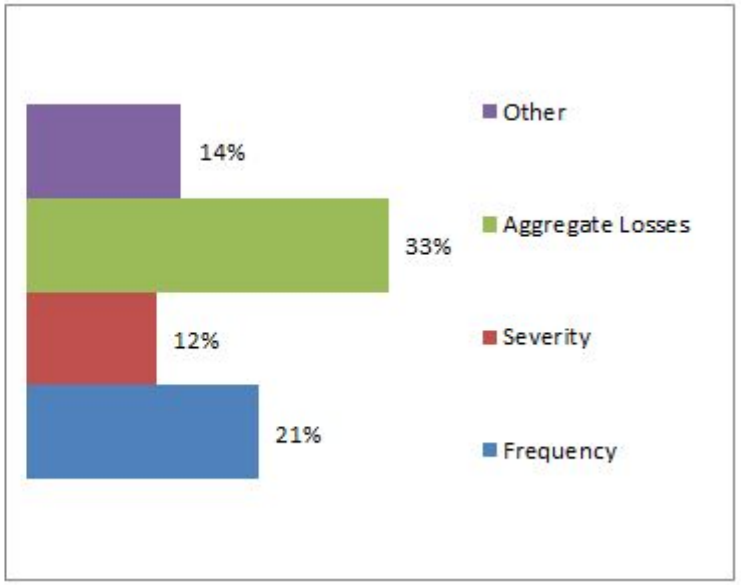
Loss aggregation options

- Gaussian copula
- Gumbel copula
- Correlation matrix









SOURCE:
1. Observed range of practice in key elements of Advanced Measurement Approaches (AMA). BCBS, July 2009
2. Carol Alexander. Operational Risk: Regulation, Analysis and Management, Pearson Education, 2003

Table of Contents

Pillar II. Risk Measurement and Analysis

1. Risk event data collection
2. Capital Requirement
3. Scenario analysis

SOUND PRACTICE

Basel Committee on Banking Supervision

> Principles for the Sound Management of Operational Risk, June 2011

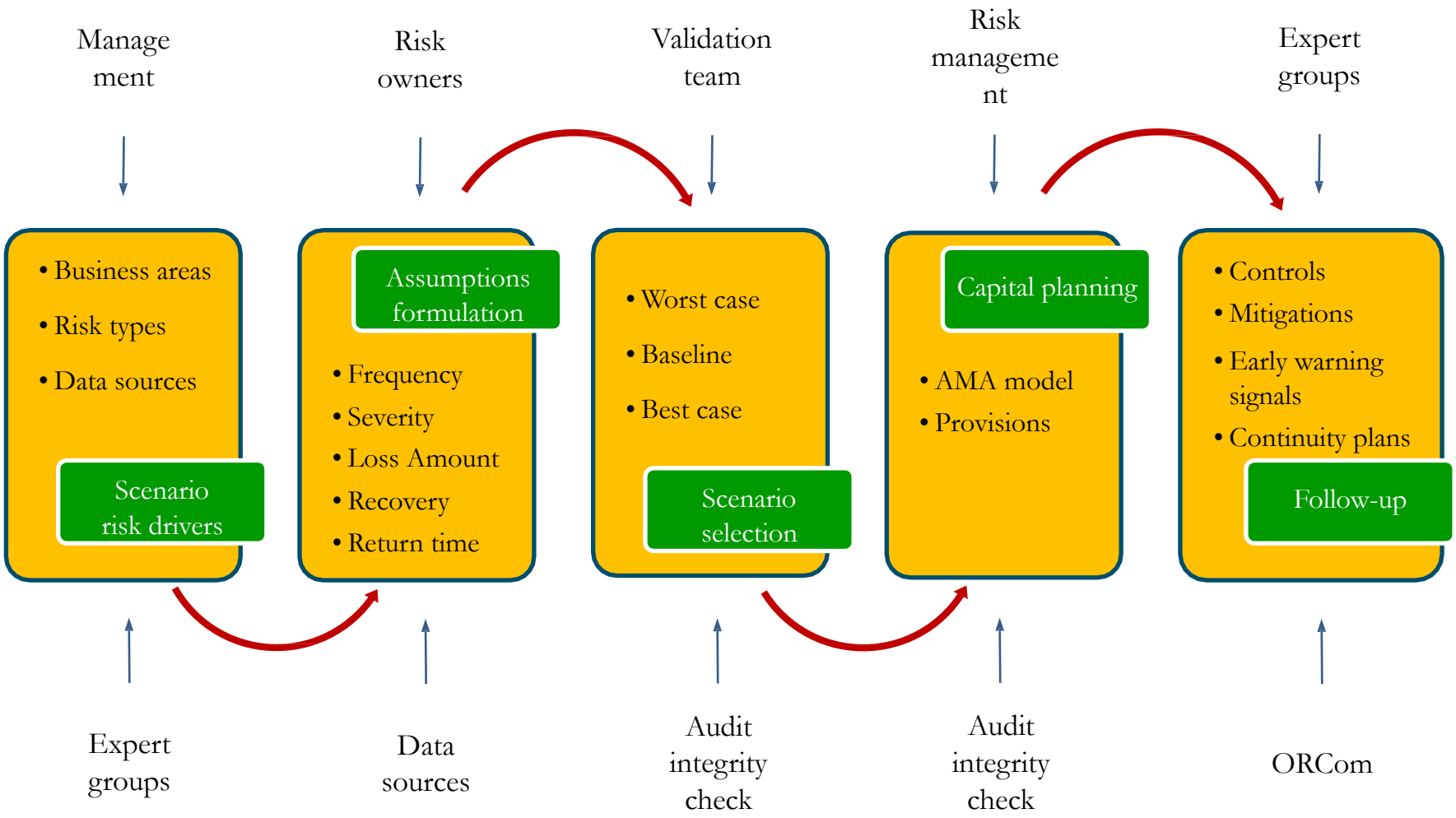
Scenario Analysis is listed as an example of tools that may be used for identifying and assessing operational risk:

—Scenario analysis is a process of **obtaining expert opinion** of business line and risk managers **to identify potential operational risk events and assess their potential outcome**. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process‖

> Basel II Framework:

Scenario analysis is a part of AMA quantitative standards: —A bank must use scenario analysis of expert opinion in conjunction with external data **to evaluate its exposure to high-severity events**‖

SCENARIO ANALYSIS PROCEDURE

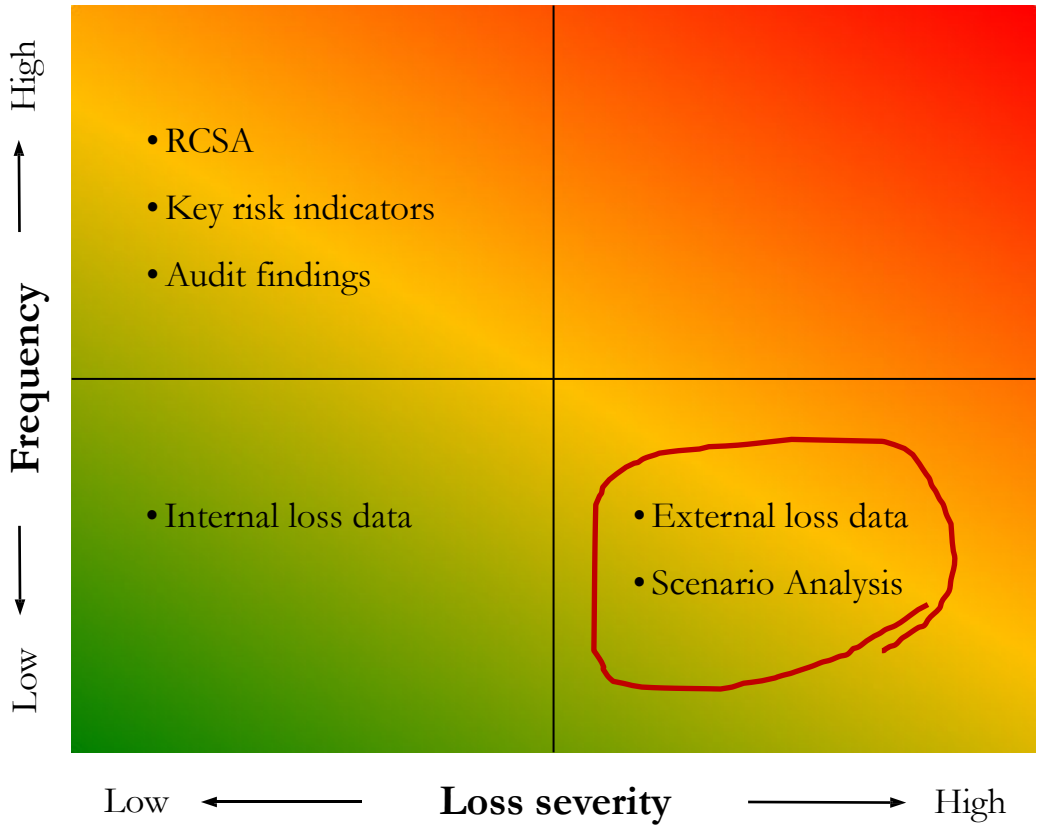


WRITING SCENARIOS ALGO

1. Defining and structuring the task, specifying the area of interest and identifying the major relevant features of this area.
2. Describing important external factors and their influence on the area of interest. These factors form the influence fields.
3. Identifying major descriptors for each field and making assumptions about their future trends.
4. Checking the consistency of possible combinations of alternative assumptions regarding the critical descriptors and identifying assumption bundles.
5. Combining assumptions with the trend assumptions regarding the uncritical depicters, resulting in a scenario for each field.
6. Making assumptions with respect to possible interfering events and their probabilities as well as their impacts on the field.
7. Assessing the impact of the field scenarios on the area of interest and its depicters. Respective scenarios are constructed.
8. Identifying strategies that could promote or impede the developments described in the scenarios.

SOURCE: Imad A. Moosa. Operational Risk Management. Palgrave Macmillan, 2007

WHAT SCENARIOS ARE RELEVANT?

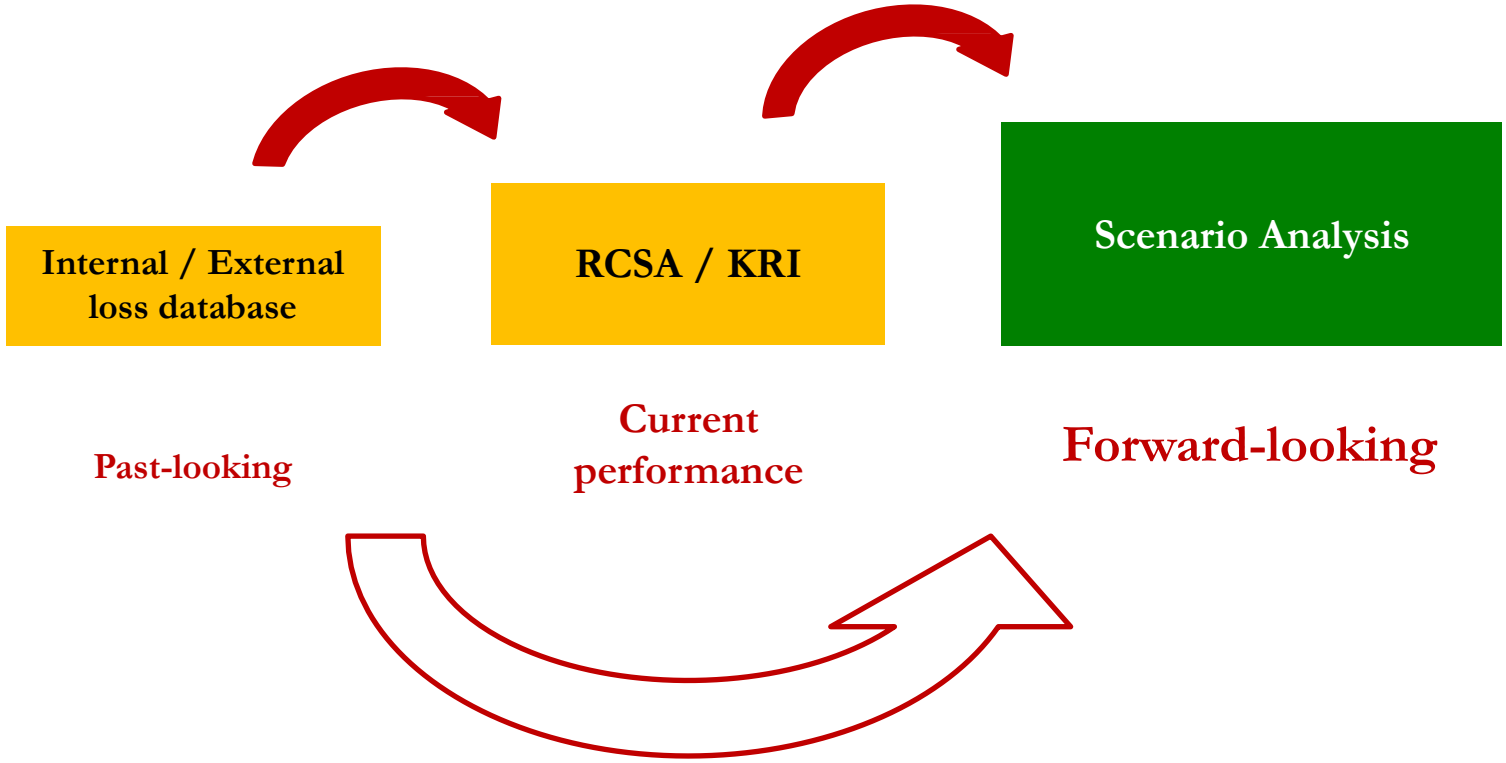


Scenario requirements:

- ✔ Low frequency
- ✔ High severity
- ✔ Realistic to the company

FORWARD-LOOKING FOCUS

Scenario data provides a **forward-looking view** of potential operational risk exposures, based on historical or judgmental estimations.



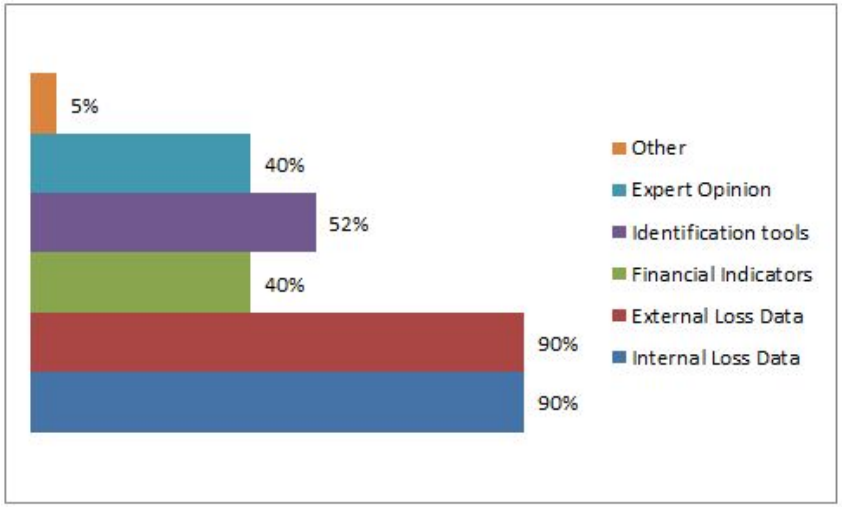
DATA COLLECTION (1/2)

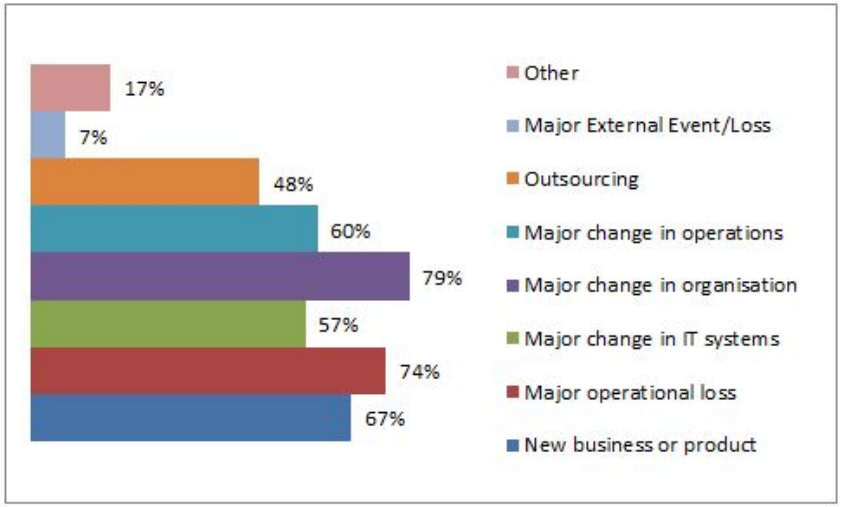
Data sources

- External loss data
- Internal loss data
- KRI / KPI
- RCSA
- Expert opinions (imaginative thinking)

Data types / updates

- Major changes
- Extreme losses
- At least annually revised





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

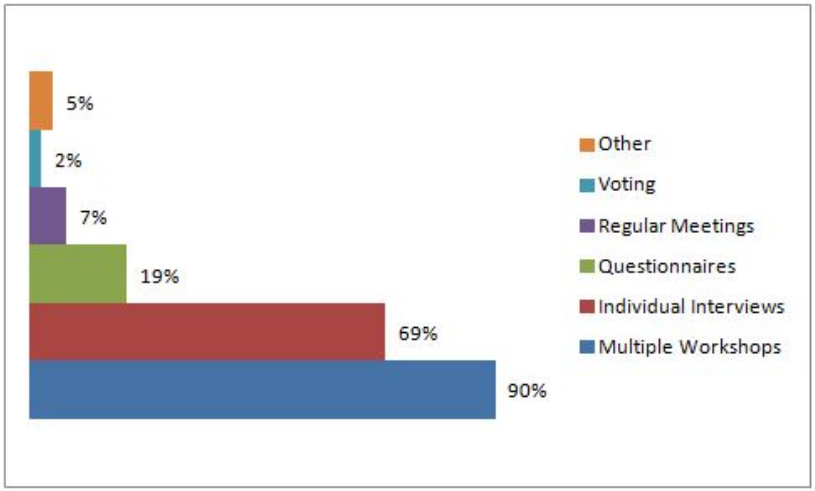
DATA COLLECTION (2/2)

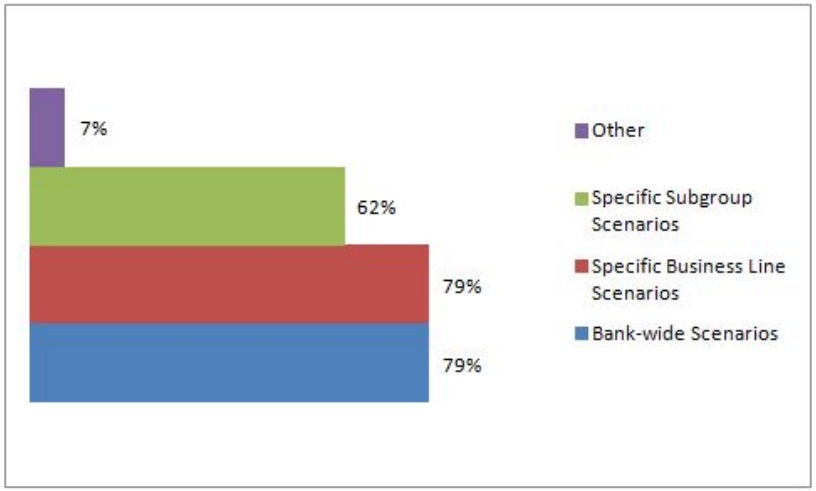
Collection process

- Workshops (expert group)
- Interviews (business lines)
- Questionnaires (business lines)
- Regular meetings (ORCom)
- Voting (expert group)

Data scope

- Bank-wide scenarios
- Business line scenarios
- Subgroup scenarios





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

SCENARIO RISK DRIVERS

RCSA may help to identify the business lines and event types of high impact

	Internal fraud	External fraud	Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption and System Failure	Execution, Delivery & Process Management
Corporate Finance	Failure to follow procedures/limits	Misrepresentation of information	Occupational accident	Regulatory breach	Business continuity failure	IT system failure	Transaction error
Trading & Sales	Unauthorized trading	Forgery	Occupational accident	Compromised client information	Damage to premises	IT system failure	Data entry error
Retail Banking	Embezzlement	Credit card robbery	Environmental issue	Negative media publications	Terrorist attack	Utility outage	Inaccurate/Incomplete contract
Commercial Banking	Theft of customer funds	Fraudulent transfer of funds	Discrimination	Client suitability	Natural disaster	IT system failure	Lost loan documentation
Payment and Settlement	Theft of client funds or assets	Payment fraud	Discrimination	Noncompliance with AML rules	Business continuity failure	Failure of payment channels	Failure to follow procedures
Agency Services	Abuse of duties	Forgery	Wrongful termination	Mis-selling	Business continuity failure	IT system failure	Processing error
Asset Management	Unauthorized trading activities	Cybercrime	Occupational accident	Fiduciary breach	Business continuity failure	IT system failure	Mismanagement of account assets
Retail Brokerage	Insder trading	Forgery	Occupational accident	Compromised client information	Business continuity failure	IT system failure	Tax noncompliance

SCENARIO DISTRIBUTION

Aggregate Number of Top 20 Scenarios
by Business Line and Event Type

Business Line	Event Type								Total	Percent of Total
	Internal Fraud	External Fraud	Employ-ment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption & System Failures	Execution, Delivery & Process Manage-ment	Un-allocated		
Corporate Finance	7	8	1	26	5	1	10	1	59	5%
Trading & Sales	31	6	2	24	7	11	21	0	102	8%
Retail Banking	40	40	7	65	27	29	49	1	258	21%
Commercial Banking	16	10	1	30	5	7	44	0	113	9%
Payment & Settlement	10	6	0	8	1	9	9	0	43	3%
Agency Services	11	6	1	14	1	21	26	0	80	6%
Asset Management	10	4	3	16	4	3	22	0	62	5%
Retail Brokerage	12	4	2	15	5	4	12	0	54	4%
Unallocated	69	43	36	78	88	49	90	17	470	38%
Total	206	127	53	276	143	134	283	19	1,241	100%
Percent of Total	17%	10%	4%	22%	12%	11%	23%	2%	100%	

SOURCE: Results from the 2008 Loss Data Collection Exercise for Operational Risk. BCBS, July 2009

HIGH SEVERITY SCENARIO EXAMPLES

- Large loan or card fraud (internal / external)
- High-scale unauthorized trading
- Legislation non-compliance or incomplete disclosure (banking, tax, AML regulation)
- Massive technology failure or new system migration
- Servers disruptions / network shutdown that lead to outages and loss of information
- Mergers and acquisitions with other banks
- Doubling the company‘s maximum historical loss amount
- Increase/decrease of loss frequency by 20%
- Increase/decrease if loss severity by 50%/100%

SOURCE:

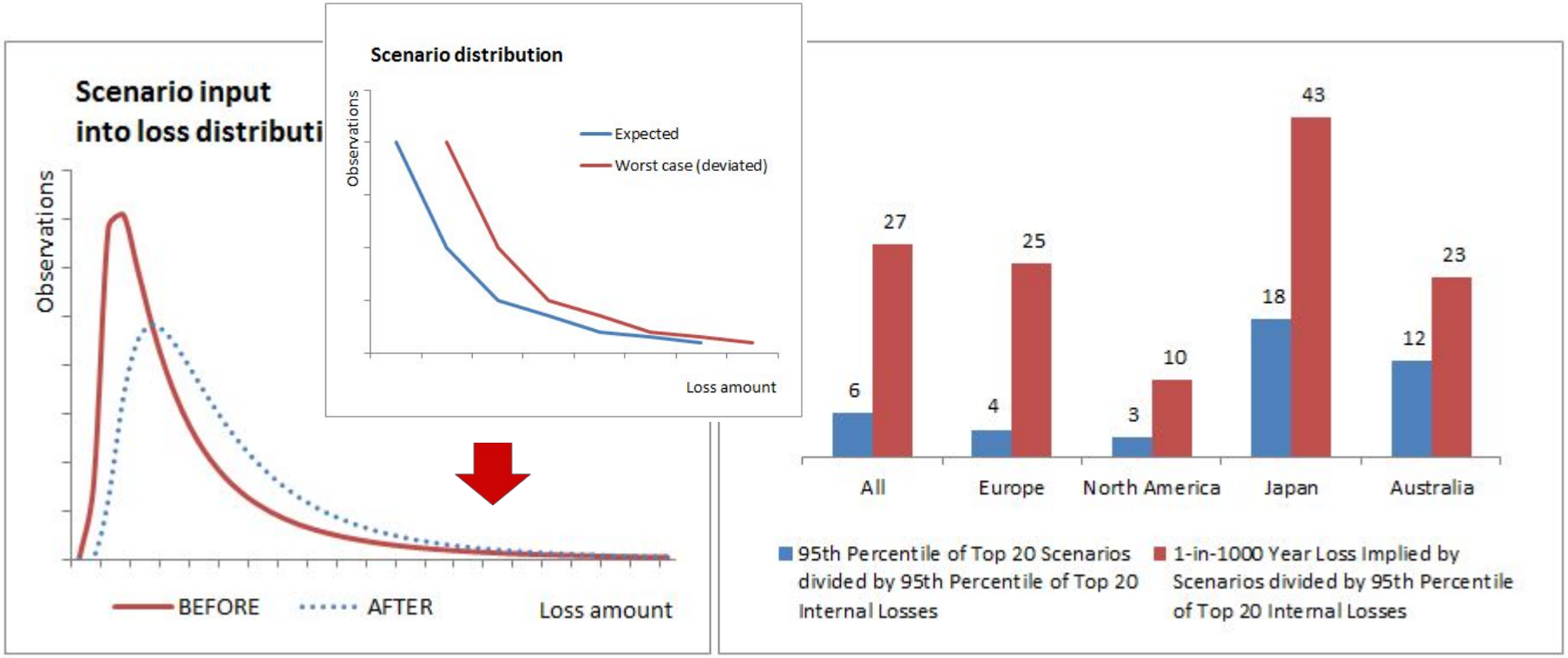
Anna S. Chernobai, Svetlozar T. Rachev, and Frank J. Fabozzi. Operartional Risk: A Guide to Basel II Capital Requirements, Models, and Analysis. Wiley Finance, 2007

SCENARIO PARAMETERS

Parameters Name	Parameters Value				
	Likely	Unlikely	Very unlikely	Rare	Impossible
Scenario Name	Large-scale payment card client data compromising				
Scenario Data Source	External loss data				
Business Line / Unit	Retail Banking / Payment cards servicing department				
Risk Type	External fraud on payment cards				
Risk Object	VISA payment cards				
Effects	Client funds are stolen with Internet payments				
Exposure	100 cards	500 cards	5.000 cards	50k cards	500k cards
Frequency (times per 10 yrs)	20	10	5	2	1
Severity	€100K	€500K	€5M	€50M	€500M
Uncertainty (std)	€10K	€100K	€2M	€25M	€300M
Controls	Suspending operations in 5 minutes after massive withdrawals				
Mitigations	Default limits on one-off and daily payments, Verified by Visa service				
KRIs	Number and severity of fraud events on payment cards				
Loss experience	…				

QUANTIFICATION USE

- ✔ Scenario estimates should add high frequency, but low severity internal loss data
- ✔ Scenarios account for 93.8% of the total number of high impact losses
- ✔ Scenario loss severity is 3-5 times higher internal loss data severity



SCENARIO BIASES (1/2)

Overconfidence: underestimation of risk due to the number of observed events being small

Availability: overestimation of events that respondents had closer or more recent contact with as personally experienced events are usually more prominent, as are events occurring more recently

Anchoring: When people are asked to estimate range for uncertain, they use a starting point (anchor), and this may create a tendency for experts to overestimate success and underestimate failures

Motivation: misrepresentation of information due to respondents' interests in conflict with the goals and consequences of the assessment

Partition dependence: refers to whether the respondents' knowledge was distorted by discrete choices of responses had to be represented, which may lead to underestimation of low frequency events and overestimation of high frequency events depending on expert experience

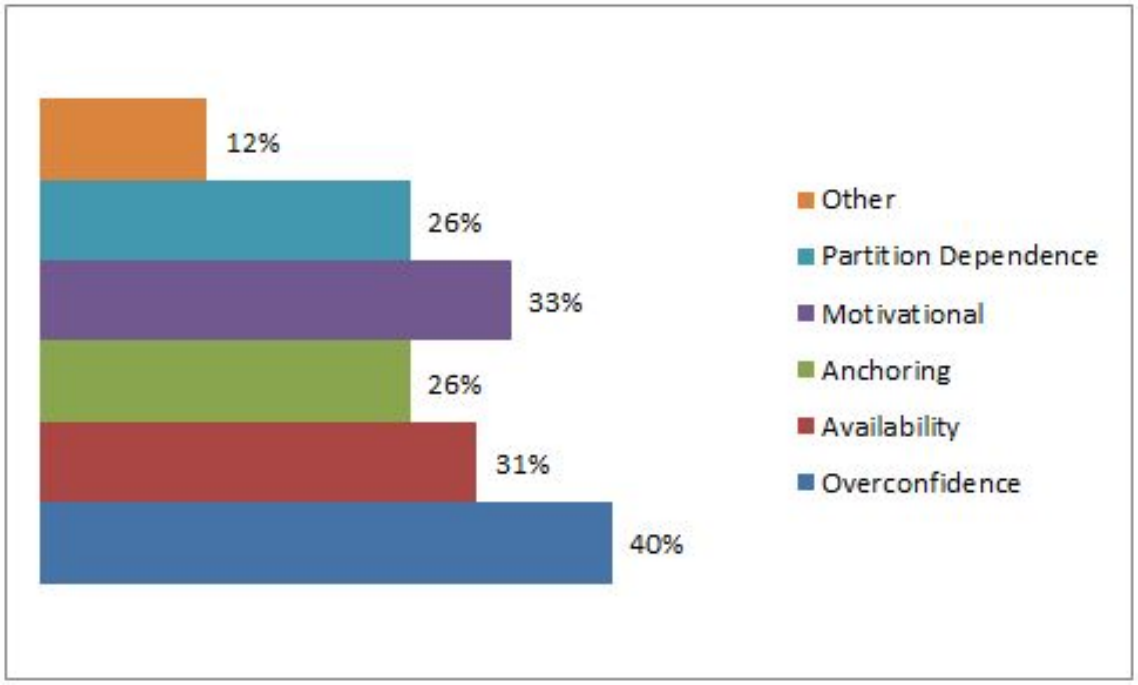
Framing: outcomes from questionnaires are sensitive to the phrasing and the order of questions used

Representativeness: experts may tend to link events they are asking with another similar event and derive their estimate from the probability of the similar event

SOURCES:
1. BCBS. Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, June, 2011
2. Greg N. Gregoriou. Operational Risk toward Basel III. Wiley Finance, 2009

SCENARIO BIASES (2/2)

Banks are likely to deviate from true risk estimate due to low frequency of events, too much rely on recent data, and conflict of interest



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

ROBUST FRAMEWORK

Established scenario framework should ensure the integrity and consistency of the estimates produced with the following elements:

a) Clearly defined and repeatable process
b) Good quality background preparation of the participants
c) Qualified and experienced facilitators
d) Representatives of the business, subject matter experts and risk managers
e) Structured process for the selection of data fore scenario parameters
f) High quality documentation of the scenario formulation and outputs
g) Robust independent challenge process and oversight by risk management
h) Process that is responsive to internal and external changes
i) Mechanisms for mitigating biases inherent in scenario processes

SOURCE: Basel Committee on Banking Supervision.
Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, June, 2011

Table of Contents

Table of Contents

Pillar III. Management Actions and Framework

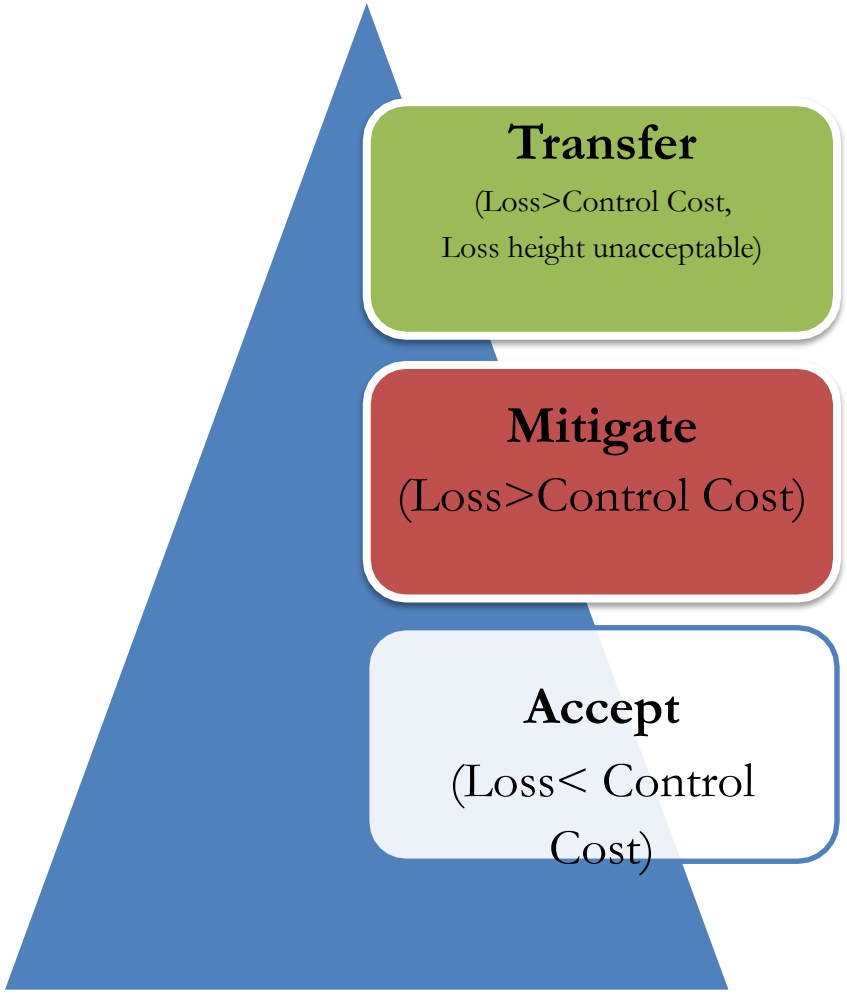
RISK TAKING & MANAGEMENT OPTIONS

Profit>Risk Cost

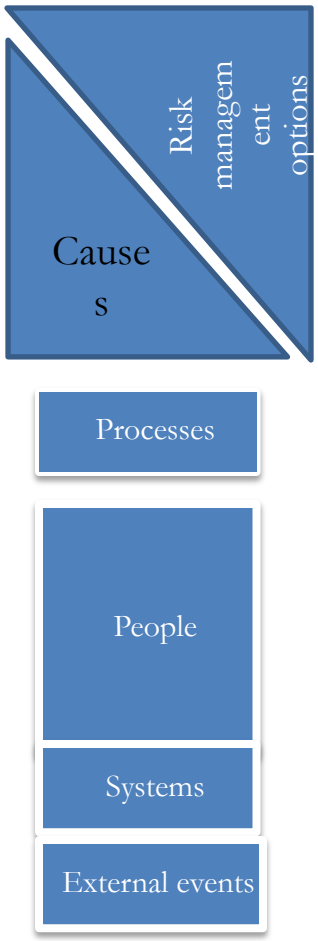
- =>Perform activity
- => OpRisk taking

Profit<Risk Cost

- => abandon activity
- => Risk avoidance



OP RISK MITIGATION



Mitigate

Automatisation,
Check sums, Plausibility checks

Trainings, separation of functions
Satisfaction , need-to—known principle (access control), 4-eye principle, physical access control...
Limit management
Inventories, plausibility checks

Backup systems
Parallel systems

Business Continuity Planning

BSBC PRINCIPLE 10: BUSINESS RESILIENCY AND CONTINUITY PLANNING

BC-Plans shall take into account different types of likely or plausible scenarios to which the company may be vulnerable.

- **Continuity mngt incorporates:**

(1) Biz impact analysis;

(2) Recovery strategies,

(3) testing, training and awareness, communication programs,

(4) Crisis mngt prgrms

- **Banks shall identify critical biz operations and key internal and external dependencies and appropriate resiliency levels/.**
- **Biz continuity testing with key service providers recommended.**

BUSINESS CONTINUITY PLANNING

BCP = disaster prevention & disaster recovery planning.

Disaster prevention aims to reduce threats of disaster before it occurs.

Disaster recovery seeks to re-establish the critical functions after an interruption / disaster.

4 core resources to be protected:

-people;

-location;

-IT; and

-external services

Efficient management of disasters – arguably more **important** to stakeholders than risk transfers.

Consists of developing for each business and support line of

- Structures
- Procedures
- Methods

To be implemented in the event of "disaster" resulting from

- Natural cause
- Accidental cause
- Voluntary act or obstruction

In order to protect

- 4 core resources
- Ensure the provision of essential services
- Ensure the resumption of all activities

…and face threats of different nature (natural, technical, malicious etc)

BCP PHASING

Phase 1: Project Planning

- Identify disaster scenarios to be addressed
- Develop Standards and Procedures.
- Establish and obtain approval on scenario and planning assumptions
- Adapt methodology tools to your culture and requirements

Phase 2: Biz Impact Analysis

-Map processes

-Assess financial and non-financial impact of risk

- Determine recovery time objective

- Determine critical processes requiring planning

- Tools, resources, equipment

- Identify key dependencies

Phase 3: Recovery Strategy Selection

Consolidate and finalize recovery requirements;

-Review and assess current strategies;

-Recommend recovery strategies

Phase 4: Development & Documentation

•Develop Crisis Management Approach and BCPs.

•Validate critical processes, and applications and map to IT infrastructure.

• Validate critical data and associated risks.

•Validate key internal and external dependencies..

Phase 5: Testing & Implementation

- Conduct structured walkthrough for each plan incl. execution of Crisis Management Approach.

• Finalize BCPs

• Develop Testing and Maintenance Guidelines and tools.

BCP SCENARIO/RISK ANALYSIS BASED

Scenario & Risk Analysis

Health Check of Physical & IT Security Controls; Threat Analysis; Review Existing Mitigation Program (evaluation of EXTREME vs MUNDANE risks)

Tools: Checklists:
1) Health
2) Risk Assessment

Business Impact Analysis

Determine (core) business processes – rank mission critical criteria; determine fin & op impacts of business process failure; recovery time objectives and interdependencies among projects

Deliverable: BCP Workbook

Recovery Strategy Selection

Min recovery resources; Range of strategies; Cost/benefit review

Tools: Industry Benchmarking & Best Practices

Tools:
TOR; Resource & BCP Templates;
Deliverable: BC-Plan

Recovery Plan Development

Prepare team procedures; Prepare team structures, Draft BCP

Deliverables:
Testing&Maintenance Procedures; Testing Summary Report; Revised BCP

Testing & Maintenance

Test & Maintenance procedures;

Document final BCP; Structured walk-thru

CRISIS MANAGEMENT STRUCTURE

Roles & Responsibilities ought to be defined in the Crisis Mngt Policy

Principles of the Crisis Management to be established & applied:

- Protection& safety of staff;
- Operational collaboration;
- controlled process of information flow;
- Maintaining essential controls in crisis situation.

Roles	Responsibility
Crisis Director (heads the crisis mngt cmte and steers thru the crisis)	▪Confirms the crisis status & level ▪Decides on the mobilization of a crisis cell ▪Expresses external resources requirement; ▪Indicates functional dep'ts likely to be affected
Crisis Mngt Advisors (members of crisis mngt cmte)	▪ Assist the crisis director; ▪ Contribute tech & organizational knowledge to handling the crisis
Crisis Communication Mngr (CMC member)	Suggests communication actions & strategies; Interfaces with the communication sector
Crisis admin & logistics	Administers documents of the crisis cell; Runs the logistics of the crisis cell

PERIODIC BCP CHECKS

1. BCP ought to fit the activity, prioritizing the core ones.
2. BCP covers all essential business processes, locations, facilities
   (incl. shared ones) and data (electronic & paper).
3. How often / thoroughly are BCP procedures tested and rehearsed?
4. Is BCP regularly updated in line with transformation projects?
5. Is “backup to backup” needed?
6. Test from your back-up to your bizpartners back-up recovered environments.
7. Is BCP internally audited?
8.

BCP TIPS

- Simple preventive measures – geographic dispersion of intellectual capital;
- Implement alternative IT solutions for communication & connectivity
- Contact details of CMC members shall be known;
- Crisis operation sites shall be equipped;
- Multiple locations, as per risk assessment, need to be prepared
- Leverage BCP budgets to address multiple business & technical needs (e.g. data backup/records management, system redundancy/performance mngt)
- Focus on pre-event risk minimization and post-event response strategies
- Plans should cover crisis management, recovery and involve all parts of the organization
- Keep plans simple – as they to work in the heat
- Really understand vendor & business partner recovery capabilities.

RISK TRANSFER

Causes \ Risk management options	Insure	Outsource	ART
Processes	X E.g.: Vault transport of cash	x	
People	X Bankers professional indemnity (mistakes by employees) Directors and offier liability Employment practice liability (e.g. discrimination) Economic crime Unauthorised trading	x	
Systems	X Business interruption Computer crime	x	
External events	X E.g. Property insurance		x

INSURANCE

Benefit:

Helps removing OpRisk from the balance sheet for a small cost (premium) by providing a restrictive cover and (un)certain payment.

OpRisk **substituted** with a counterparty/credit risk on an insurer.

Questions of Insurer's liquidity, loss adjustment, voidability, moral hazards, limits in insurance product range.

9/11 and Moscow **terrorist** attacks called to rethink insurability conditions and identify hidden exposures. Terrorism magnifies business interruption as a major OpRisk.

Insurance does not protect reputation or ensure that business can continue

Challenges of using the insurance:

-Selecting the right coverage

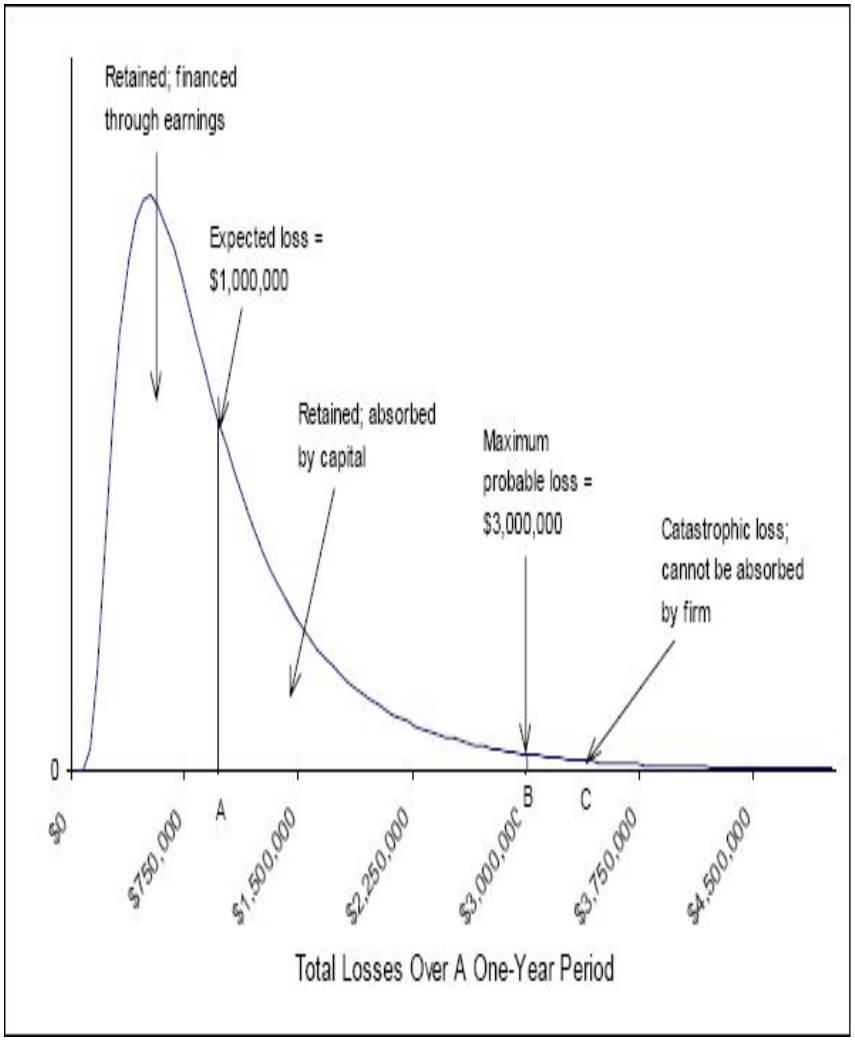
-Incorporating the insurance policies into the capital allocation strategies;

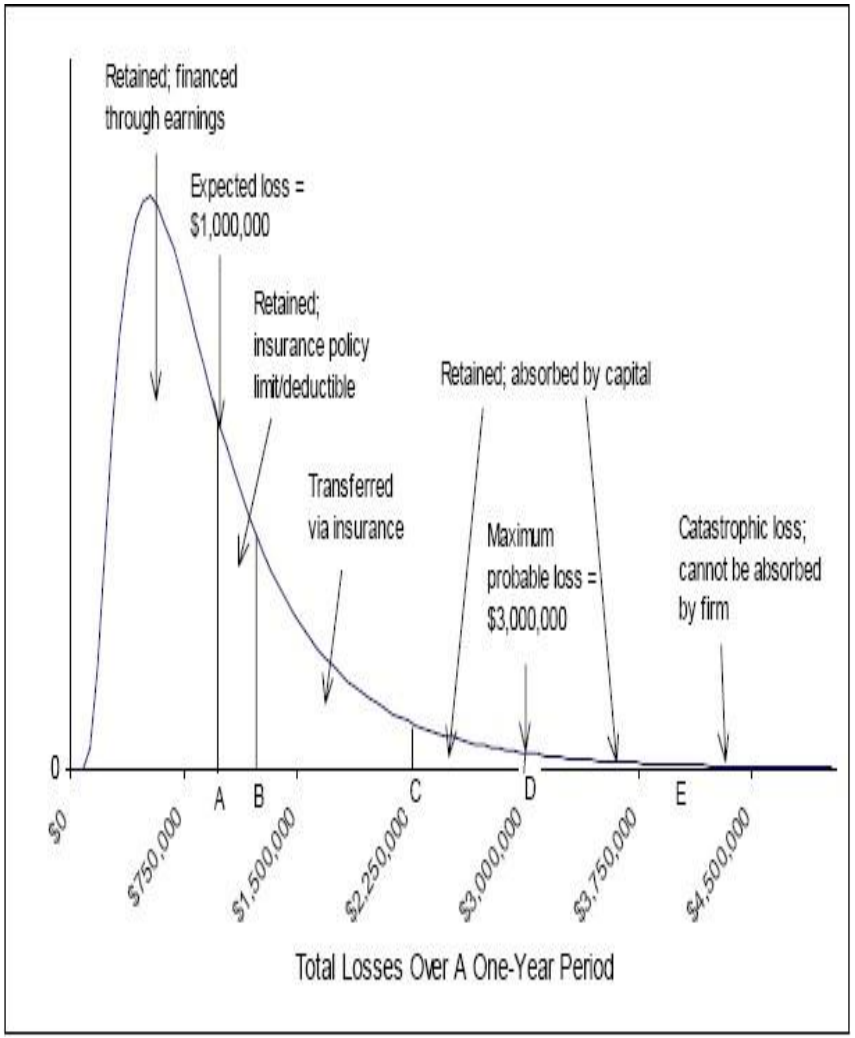
- potential payment delays (critical for small credit institutions

Conditions:

- Must be related to actual risk exposure of bank to evidence need for mitigation, (e.g. catastrophe insurance in case of earthquake)
- Insurance provider rated at least A
- Insurance provider not to be related to banking group; unless re-insured via eligible re-insurer
- Tenor of insurance 1 year for 100% recognition
- If less than 1 year, apply haircuts, to reach 0% recognition if under 90 days
- No exclusions or limitations as a result of regulatory action or events that took place before insolvency

INSURANCE MITIGATION UNDER AMA





OUTSOURCING RISKS

Op Risk Outsourcing drivers

- Cost reduction
- Higher process quality
- Risk sharing/ transfer
- Benefits from economies of scale;
- Allowing better focus on core/new business;
- Accessing new technology

COMPETITIVE EDGE –OUTSOURCING IS NOT OR-FREE

Outsourcing OpRisks:

(1) Unavailability of critical systems / loss of data

(2) Legal risks with the segregation of duties. Who bears losses?

(3) Loosing control over the process.

(4) Black-Box systems: Loss of know-how; dependence on key personnel

(5) Reputation risks in case of poor service

(6) Compliance risks (e.g. customer data protection)

(7) Counterparty risk: (business partner_s failure on service delivery), incl. fraud.

BSBS —Outsourcing in Financial Services‖ – Feb 2005.

"Prudent Outsourcer" Rules

1. The final responsibility towards clients and supervisors for the outsourced service remains with the financial institution. While an operation / service may be outsourced, the ultimate responsibility for it – not.
2. Focus on core activities, gaining efficiency and saving cost shall outweigh the loss of direct control over the service and be based on the provider assessment.
3. Outsourcing causes loss of know-how, information and some infrastructure.
4. Key processes and core competencies shall not be outsourced.
5. Min quality and reliability expectations, ability to provide KRI's / KPI's and securing confidentiality as per Service Level Agreements.
6. Outsources shall make sure the insourcer has adequate safeguards in place. Really understand vendor / business partner recovery capabilities
7. The out- and insourcer's duties shall be segregated.
8. Manage reliance on external entities (risk of failure)
9. Open communication channels btw out- and insourcer and auditing rights and sufficient process control rights.
10. Instill satisfactory management report.
11. Reduce degree of dependence: can bank switch outsource provider if fails (backup provider)?

ART
(Alternative Risk Transfer)

Regulators concerns:

-Complex voidance clauses

-narrowly defined insured / risk events

Limitations

-Absence of historical data

-Imperfect knowledge in certain domains on the part of actuaries

Products	Product distinctive Features
Insurance-linked securities, incl. index securitization	Supercatastrophes
Finite reinsurance Risk transfer + risk financing	- Multi-year; -particulars of each oprisk covered; -Possible sharing of fin results
CAT(astrophe)-bonds	If no loss-event occurs, investors receive coupon If a defined catastrophic event takes place, investors lose interest, principal or both
Catastrophe swaps	Fixed payments exchanged for a series of floating that depend on occurrence of an insured event
Industry Loss Warranties	Resemble catastrophe swaps, structured as a reinsurance
Catastrophe options	Listed at Chicago Board of Trade

Table of Contents

Pillar III. Management Actions and Framework

OpRisk CORPORATE GOVERNANCE

Clear org structure with defined lines of responsibility

Hierarchic decision-making process

Adequate Internal Control Structures proportionate to the scale of Bank‘s activities

Output of RM system must be integrated into the controlling of operational risk profile

Internal & External Assessment to Ensure the ORM framework fits the purpose

RISK GOVERNANCE: 3 (4) LINES OF DEFENSE

Role of Supervisors

-Conduct regular independent evaluations of banks' OR policies, processes & systems

-Ensure Compliance with the Principles at the Financial Group level;

-Address deficiencies through the range of actions;

-Benchmark risk mngt plans to others';

-Applicable to all Banks regardless of size

… and regulatory expectations

-evolve as the institution gains experience with RM techniques;

-**RM Enhancement;**

- Evidences ORM benefits to banks

(1) bizline mgnt have primary responsibility for managing their risks (**Risk-takers**);

(2) independent corporate ORM function – supports the line mngt; responsible for **risk oversight** and guidance;

(3) Independent **assurance**, consists of *verification* (tests the efficiency of the overall framework) and *validation* (ensures the robustness of quantification s-ms) – internal /external audit;

arguably, the Board of Directors shall form the last internal line of defense

RISK MANAGEMENT ORGANIZATION

Bank RM Function	Centralized	Distributed	Decentralized
Relation to the business	ORM Officer/Cmte; No dedicated bizline support	ORM Officer/Cmte +Bizline ORM Managers &/or dedicated staff	largely independent RM programs managed by bizlines
Responsibilities	Identifying and managing risk at central level	Identifying and handling risk devoted to central functions; identification of ORs is with bizlines; Meets specific OR requirements of each bizline	Identifying & managing risks at BizLine level; Handling certain risks centrally; functional reporting of bizline risk managers to ORM
Pro's	Standard approach to risk identification & mngt; consistent mngt info	Risks identified by biz transactors; standard approach to risk mngt;	Risk identification by biztransactors; ownership with risk takers; selective use of centralized risk handling measures; generation of complete MI
Con's	No bizline ownership; lax risk-identification; Incomplete MI	Lack of ownership by risk takers to manage; Unacceptable risk taking	Inconsistent standards & procedures (mitigated thru clear guidelines and their monitoring)

OpRisk GOVERNANCE INTERNAL STRUCTURE

Element	ORM Tasks & Responsibility
1. Supervisory Board	Approves and periodically reviews operational risk management strategy Receive reports on OR exposure against risk appetite, Aware of major OpRisks and significant losses; Ensures Management Board carrying out its responsibilities
2. Management Board	Responsible to implement risk mgnt strategy Approves and periodically reviews the oprational risk framework Ensures the staff across the organization are clear as to their roles in ORM Ensures appropriate action taken in response to OR exposures exceeding the appetite; Launches and manages projects for operational risk management (incl. its budgeting, resourcing and awareness campaign);
3. CRO (often a Board Member)	Responsible for implementation of OR framework Provide risk leadership, vision and direction Develops a supporting infrastructure; Sponsor for operational risk project; Internal ORM knowledge management Oversight / control of ORM
4. ORM function (Independent but not isolated from biz lines!)	Implement the ORM framework Create the tools to manage it (risk policy, monitoring, assessment, systems, methods) Ownership of guidelines and methods Identify, assess and analyze key risks Monitor risk exposures against risk appetites
5. (Operational) Risk /Audit committee	High-level technical issues Monitoring implementation of risk policy and strategy Measures to improve quality of risk management Review the results of the risk assessments and make recomendations on the OR matters

OpRisk Governance Support

Element	ORM Tasks & Responsibility
6. Line management	**Staff in bizline to operationalise control functions Coordinators between business units and risk controlling**
7. Internal auditors	Advisors and internal reviewers for operational risk projects Not responsible for OR as this would violate their business process independence Audit reports identify areas of high operational risk Assessment of quality of loss database
8. Compliance and other risk oversight functions (treasury IT sec„ty, HR)	Specialised control function to avoid insider trading, conflict of interests, monitor staff transactions
9. OpRisk coach (optional)	Consulted for private assesment of measures to build-up the RM corporate culture

SPECIAL ROLE OF RISK FUNCTION

Policy	Develop, adapt & maintain with business;
Monitoring	Develop & maintain a reporting framework. Monitor & report portfolio exposures and risk concentrations. Report and aggregate risk mngt info. Link to regulatory requirements.
Assessment	Develop & maintain risk profiling & (self)assessment program. Analyze independently.
Systems	Develop & maintain risk reporting systems with relevant biz functions
Methodology	Develop risk quantification methods and capital allocation models Transaction failure analysis, external fraud response, AML, info security, compliance.
Other (optional)	

RISK GOVERNANCE ELEMENTS

Risk identification	-Identify inherent risks in all products, activities, processes and s-ms; - Adequate assessment procedures for new products… systems.
Risk measurement	Limits & escalation process RCSA KRI Incident & loss reporting Capital allocation
Continuous monitoring	OR exposures by major biz lines OR events and losses by major business lines
Control & Mitigation	Policies, processes and procedures Cost & benefits of alternative risk mitigation OR exposure adjustment in light of overall risk profile
Audit	ORM shall be subject to regular reviews by internal/external auditors
Information flows	Enable: -sr mngt to monitor the effectiveness of ORM s-m -BOD oversee sr mngt performance; -Info shall be used and acted upon

ORM GOVERNANCE FRAMEWORK

Evolving Governance Model:

(1) a central OpRisk Mngr reporting to the CRO. The role is on settling, development of tools, coordination, analysis and benchmarking as well as integration and aggregation o fof the risk-profile +

(2) Line management remaining responsible for the day-to-day risk mngt activities +

(3) Risk committies

(4) Optional: ORM coach

- **Functional units** involved in OpRisk Mngt:
  - Mngt & Fin Accounting
  - Procurement
  - Corporate Security
  - Human Resources

- **OpRisk ownership**:

(1) Risk-takers who indulge in activities leading to OpRisk (responsibility alligned with profit centers – siloed approach);

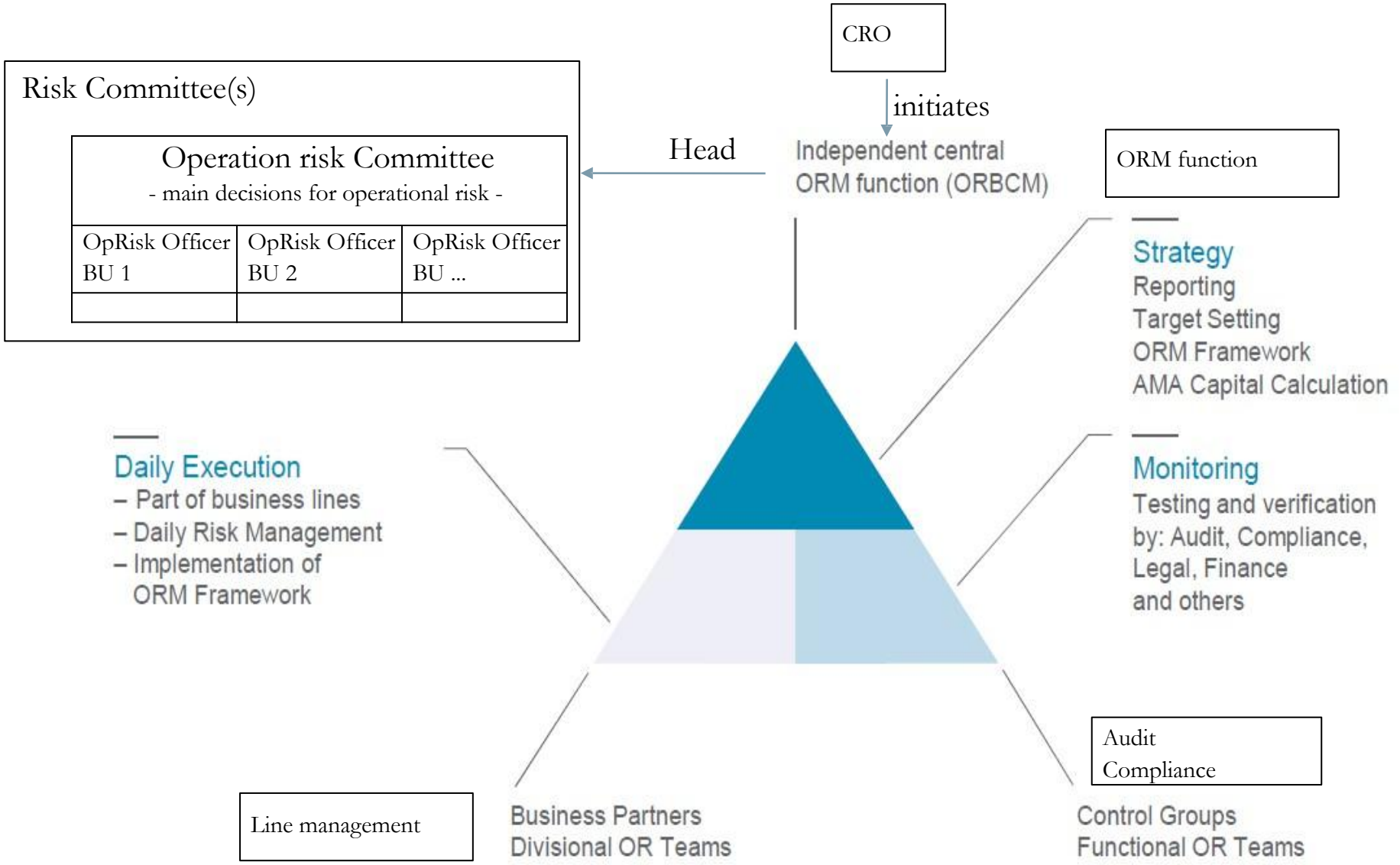
(2) A more centralized corporate body (as OpRisk is enterprise-wide).

NB! Functional support units may also generate ORs.

- Allocate OR-capital to bizlines and event types to incentivise optimising risk-adjusted capital

- OR helps to manage risks qualitatively with internal control system (e.g. capital limits) => Capital becomes an additional control variable

OR GOVERNANCE STRUCTURE: DB EXAMPLE



DISCLOSURE TO EXTERNAL STAKEHOLDERS

P11: Banks' public disclosure should allow market participants to assess its approach to OpRisk.

-Meet regulatory expectations;
-Meet ratingagency expectations (ORM assessment form part of their overall firm's assessment)

-Align business to the interests of investors; ongoing communications to ensure the investment protected;

- Effective RM leads to informed decision making

Amount and type of disclosure shall be commensurate with the size, risk profile and complexity of a bank's operations.

A formal disclosure policy shall be approved by BOD.

The Policy shall establish

(1) internal controls over disclosure and

(2) a process of assessing the appropriateness of disclosure, incl. the verification of frequency

Recommended Sources:

1) BCBS —Internal Convergence of Capital Measurement and Capital Standards: A revised framework‖, - June 2006.;
2) IOR Operational Risk Sound Practice Guidance: Operational Risk Governance, Sept 2010.

RULES OF STAKEHOLDER ENGAGEMENT

- Do internal ("machine room") and external (context) intelligence;
- Communication team composition: Experts and Message Determiners;
- Align the message with the target audience;
- separate internal and external communications in OpRisk event situation;
- coordinate & cooperate with credible sources (e.g. regulators, consultants, politicians etc);
- Cover "4 Rs" "Regret-Reform-Restitute-Responsible"
- Beware of Media mind-frames:
  - Fin institution serve ideal targets, as they deal with large sums of money;
  - Circumstances less important than victims & quantification: Simplify;
  - Deviations in size & expectations make the news (e.g. "large fraud in a trusted bank");
  - Telling a story is more attractive than a factual description.
- Protect your bank from wrong customers

- Who are your stakeholders?

-What's your Symbol (Brand, Reputation)?

- Is it worth protecting?

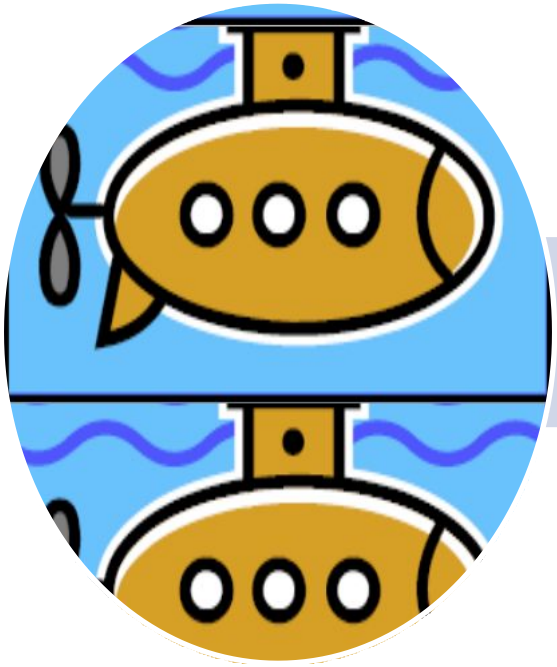
BENEFITS OF OR GOVERNANCE

- ✔ Reduction of operational losses;
- ✔ Improved business and performance management;
- ✔Protection against loss of reputation;
- ✔ Regulatory compliance;
- ✔Greater levels of accountability (staff and business unit levels);
- ✔ Reduction in regulatory capital
- ✔ Risk assessment / internal audit
- ✔New product / initiatives approval
- ✔ Strategic planning
- ✔ Systems implementation
- ✔ Outsourcing / vendor selection
- ✔Performance measurement
- ✔ Annual budgeting
- ✔Product profitability

DISCUSSION: HOW WOULD YOU RANK THESE BENEFITS?

ORM IS SIMPLY GOOD CORPORATE GOVERNANCE

Good ORM



Fewer Surprises

Increased shareholder value

Table of Contents

Contact information

INTERNATIONAL FINANCE CORPORATION (IFC)

Bank Advisory Program
Central Asia and Eastern Europe

Yevgeni Prokopenko, Banking Advisor

T: +38 095 280 5271

E: yprokopenko@ifc.org

Denis Bondarenko, Banking Expert

T: +7 495 411 7555 (ext. 2145)

E: dbondarenko@ifc.org

Thank you for time and Questions!