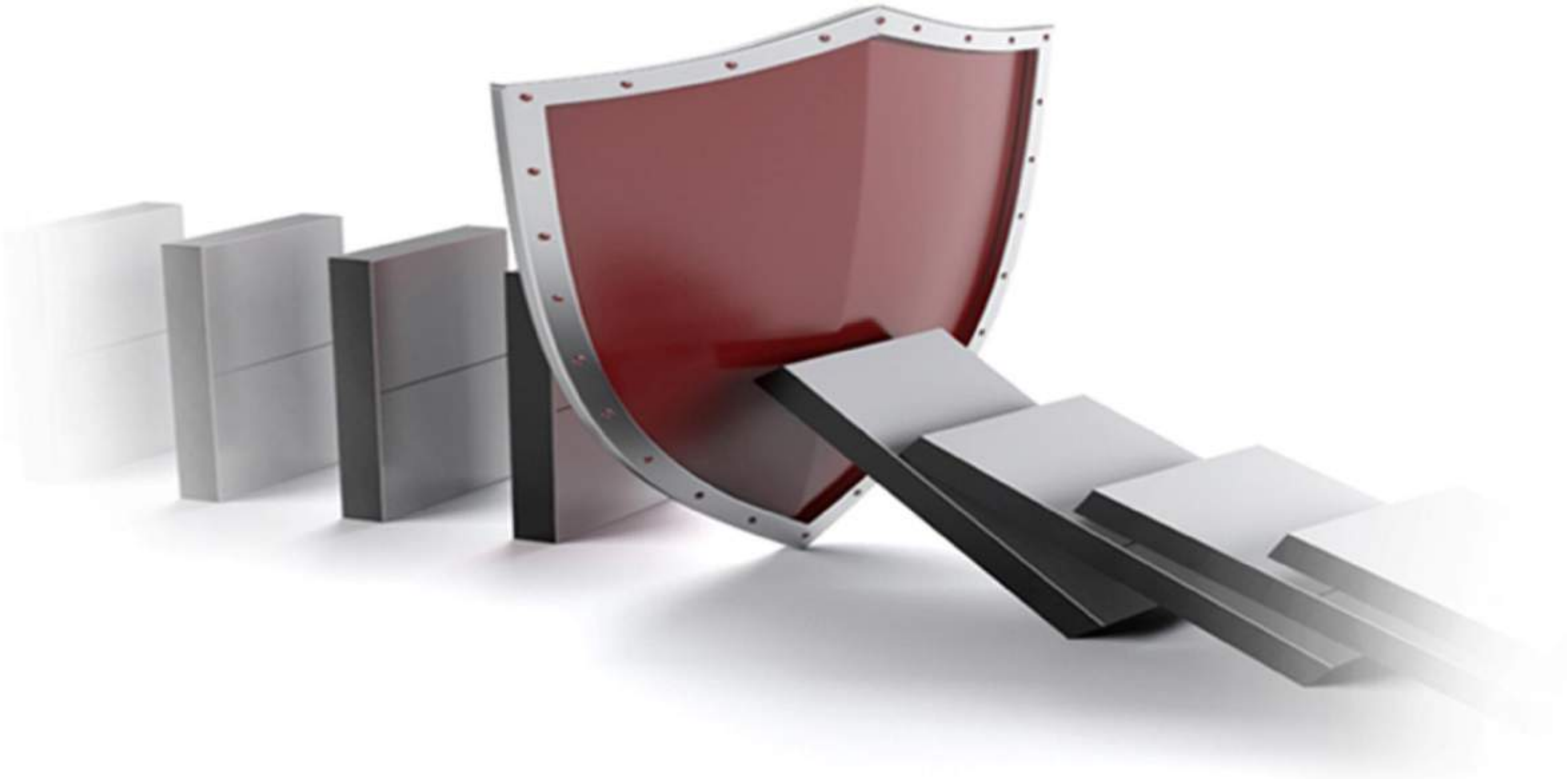
IMARTICUS MANAGEMENT DEVELOPMENT PROGRAMS



OPERATIONAL RISK MANAGEMENT

A GLOBAL BEST PRACTICES MANUAL

Dr. Ranjan Chakravarty
January, 2016

IMARTICUS
LEARNING

INTRODUCTION

The objective of this Manual is to deliver a ready reckoner to practitioners of the operational risk function for major banking institutions.

This Manual emphasizes both the concepts and techniques that are readily applicable as well as provides the background published research and the relevant regulatory reference material for the practitioner.

The Manual is indexed by topic as is the reference material. In case a reference document covers more than one topic, it is identified as such. Key takeaways are also identified by topic area.

The practitioner would find it of value to perform the exercises identified therein so as to become proficient with the techniques mentioned in this Manual.

> ***"Risk comes from not knowing what you are doing."***
>
> *- Warren Buffet*

TOPIC 1: OPERATIONAL RISK IN CONTEXT

Introduction and key definitions

Operational risk is the loss expected over the next 12 months deriving from losses resulting from inadequate or failed internal processes, people and systems or from external events.

The definition includes legal[1] risk, but excludes strategic[2] and reputational risk, according to the Basel Committee on Banking Supervision.

There is very little commonality between people or processes or IT systems or external events (such as bomb threats or power cuts). The techniques used to understand and manage operational risk are, therefore, very diverse.

Risk Drivers:
People, Processes
& Systems

Time Horizon:
Next 12 Months

In this context, it is critical to understand that operational risks are often the cause and driver of credit, market and core business or strategic risks. This means that operational risk events can have a direct or indirect impact on the value / earnings of the company or the liquidity available. For example, a direct effect of a burglary in the company building could lead to losses of stolen computer equipment. Indirect effects via market, credit or core business risks often are more severe than the direct impact if, for example, confidential data were stored on the stolen computers that subsequently get published on the internet. In rare cases such as extreme market or credit risk volatility, one could also argue that market and credit risk may be causing unexpected operational risk events because of a breakdown of the standard processes in such a period.

Distinction and relationship amongst risk types: market, credit and operational risk

It is important to understand market and credit risk in the context of operational risk, just as it is critical to understand operational risk in terms of market and credit risk.

First context is the **setting**. Whereas market risk clearly refers to potential losses from transactions with other institutions, at either exchange traded or OTC-referred recorded prices, credit risk refers to other institutions' probabilities of default either at the counterparty or issuer level, with respect to the institution concerned. However, operational risk refers to processes, people and systems within the institution itself or to exogenous events that directly impact it. Hence, it is clear that where market or credit risk can be thought of as a function of the bank's portfolio, operational risk can be thought of as a function of the bank's processes and governance.

Secondly, the **calculation methodologies** for market, credit and operational risk are vastly different.

[1] Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

[2] Strategic risks are those that arise from the fundamental decisions that directors take aiming to achieve an organization's objectives.

Market risk:

Uses transactions data

Credit risk:

Uses data that are both market and institution generated

Operational risk:

Uses data that is almost purely generated internally

The final context is **regulatory**. Methodologies for measuring and managing market risk and computing market risk capital with Internal Models – through techniques such as Historical simulation, Monte Carlo simulation or Variance-Covariance Value at Risk (VaR) – have long been accepted by regulators. Similarly, Internal Models of credit risk measurement and management, with Exposure at Default (EAD)[3], Loss Given Default (LGD)[4], Probability of Default (PD)[5] and associated methodologies are well established as of Basel II.

However, Op Risk VaR is based on the Advanced Measurement Approach (AMA). This is a nascent set of techniques which began in the Basel II regime and are in the process of being established in the Basel III world. This manual highlights the application of these techniques and provides background research on them.

Loss event types of Op Risk

The following lists the official Basel II event types with some examples for each category:

Event-Type Category (Level 1)	Definition
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/ discrimination events
Clients, products & business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events
Business disruption and system failures	Losses arising from disruption of business or system failures
Execution, delivery & process management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors

[3] Exposure at default (EAD) is a parameter used in the calculation of economic capital or regulatory capital under Basel II for a banking institution. It can be defined as the gross exposure under a facility upon default of an obligor.
[4] LGD is the share of an asset that is lost when a borrower defaults. This is an attribute of any exposure on bank's client. Exposure is the amount that one may lose in an investment.
[5] The probability of default is an estimate of the likelihood that the default event will occur.

How are different risk types measured and calculated for banks vs. other financial institutions?

Calculation of market, credit and operational risk measures and capital for banks are based on the Basel accords – Basel II and III being the versions most applicable at the current point in time.

Other financial institutions use variants. Insurance firms use Solvency II, and applied Value at Risk (VaR) techniques for buy side firms. Hence, in the banking context, we work with Basel II and III. Market and Credit VaR use a 99% level of confidence[6] unless otherwise specified; whereas operational risk calculations are at a 99.9% level of confidence.

For operational risk, using the latest version of the Basel accords, the AMA approach for a bank requires the use of four data elements which are:

Internal loss data (ILD)

External data (ED)

Scenario analysis (SA)

Business environment and internal control factors (BEICFs)

How risk paradigms vary under one umbrella?

1. **Confidence Levels:** Since confidence levels vary between 99% for market risk and 99.9% for operational risk, their aggregation into one risk capital measure is not possible. Secondly, there is a dissonance between parts of risk measurement that are based on backward-looking data as in market risk and in forward-looking and scenario based data as in operational risk. Credit risk lies somewhere in between.
2. **Distributions**: The distributions across the three types of risk vary widely. Aggregation is again not possible.
3. **Different Data Sources**: The data sources are completely different for all three risk types.

Confidence Levels for Op Risk:
99.9%

However, they all are under the responsibility of one Risk Management department, which is responsible for mitigation and risk capital allocation across all risk types and hence have to coexist under one roof as the responsibility of an independent Chief Risk Officer's domain.

Policies, procedures and metrics defined and distinguished and their contents

Policies:

1. Risk management policies are clearly dependent on the banks' risk appetite as communicated via the Board through the Risk Management Committee.
2. They are defined and communicated through the Chief Risk Officer upon the Board's approval.

[6] The level of confidence at which the institution will make the estimate. Popular confidence levels are 95 per cent and 99 per cent.

Procedures:

1. Also known as standard operating procedures, these are departmental models to implement the policies.
2. They have to be contained in approved manuals.
3. Since they are methodologies for the implementation of policies, they do not require Board approval in all cases but some might require it.

Metrics:

1. Are measurement methodologies for reporting purposes.
2. Need approval, but not necessarily by the Board, and are intended to convey various measures of risk that are being implemented.
3. They include, for example, distribution assumptions for severity, the precise formulas used and all associated formulaic details that are necessary for performing the operational risk measurement function.
4. These have to be approved, again, not necessarily by the Board, but by a senior group including the Chief Risk Officer, and form the underlying basis for the procedures.

What should each contain for operational risk?

The following documents, shared in the **Readings** section, are the relevant portions of the Basel accords referring to this section.

1. Op Risk Measurement Basel Latest Document
2. Op Risk Measurement Basel Original Document
3. Basel Principles for the Sound Management of Operational Risk
4. Principles for Sound Management of Operational Risk – Review

TOPIC 3: MANAGEMENT OF OPERATIONAL RISK

Operational risk end to end

Step 1: Identification of the Operational Risk baselines

Gap analysis for Case 1: In a first cut, a random sampling of policies and procedures was conducted. This revealed that the baseline level of policy clarity did not exist, since policies, procedures and manuals were often used interchangeably. In effect, the referencing was to itself. Often times, approvals had been taken partially, from different authorities, with authority and accountability resting with different silos.

Gap analysis for Case 2: The German bank's situation was more straightforward, with the risk in Process and Technology. Incidence and Severity data could be collected, stress tests and scenario analyses conducted, heat maps and KRIs identified and 99.9% OpVAR calculated.

Step 2: Criticality assessment

Criticality Assessment for Case 1: There had been aggressive acquisition of pricing and risk libraries from various global vendors. Most of the libraries were attached to products and systems that were desk specific and there was no clear mapping between libraries, products, systems, policies, procedures, and consequently people.

First, since gaps existed in Policy, Process and Procedure, there was no scope, therefore, of collecting meaningful loss data. Additionally, there were gaps in People and Process. Therefore meaningful operational risk management would involve revamping Policies, Processes and Procedures in addition to training People, and implementing proper Systems and Platforms, so as to collect the right data, conduct the stress tests and scenario analyses, and deliver 99.9% OpVAR for actual management.

Criticality Assessment for Case 2: The existence of efficient processes across the bank, great communication and a strong centralized Risk Management function enabled the employment of analytics, specifically those targeted at showing the 99.9% OpVAR of each business line the world over. This enabled the Risk group to conduct sensitivity analyses with Stress Tests, showing to what extent changes could drive down the 99.9% OpVAR of any or all business lines with certain mitigation measures to be taken.

Step 3: Putting in place a Business Transformation paradigm

Business Transformation paradigm for Case 1: Once the Templates, Work Flows, Policy Standards, Policy Prototypes and Platforms were finalized and signed off, the Proof of Concept was ready. It is only then that the transition could be operationalized.

Business Transformation paradigm for Case 2: The situation here was much more dependent on analytics. Once the 99.9% OpVAR data had been simulated and collated, the business lines, business units and processes where the maximum 99.9% OpVAR "payout" could be achieved were identified.

Step 4: Transition rules

Transition Rules for Case 1: At the Policy level, the scope of the Policies had to be adjusted to meet the Basel requirements. In the instances where the scope remained intact from the old dispensation to the new, then there would be no need to write a new policy. In such a case, the same policy would go to approval (again) and would be fast tracked into Process and Procedure as per the new template.

In cases of brand new policies, the entire Policy, Process and Procedure model would have to be rewritten and reapproved in sequence. Once the Policies, Processes and Procedures had been reviewed and implemented they would be considered a Prototype. It is only upon completion of this stage, and through Prototypes that the Loss data and Scenario collation stage would begin as a precursor to the calculation of 99.9% OpVAR.

Transition Rules for Case 2: Since the stage was set for operationalizing the transition to a newer and tighter level of operational risk based on the already calculated 99.9% OpVAR for each business line, the actions for system and procedure change had to be executed in a transparent and coordinated fashion across Risk Management and Tech & Ops. The transition had to be documented rigorously, and audited by Internal Audit. This was the last stage before the preparation for the Regulatory audit for the transition to Basel compliance.

Key Risk Indicators (KRIs) from actual experience

Case 3 – a global derivatives exchange and clearing house

Facts: As a first level of defense after the Regulator, exchanges are under pressure to meet best practice standards in advance of other financial institutions due their implied regulatory responsibility. As a consequence the Risk Control Self-Assessment (RCSA) or Risk Register exercise is of great importance. This is a case of such an exchange and clearing house that delivered the Risk register exercise[7] efficiently and correctly to Regulatory approval.

Step 1:

The objective of the RCSA exercise was to enable each division to participate in an assessment exercise that would enable the institution to collect accurate data. The first stage in this exercise, therefore, was a Training and Communication stage. Each department and each employee in each department was provided a "mock" template with which to enter the data. In the training, it was clearly communicated that each division would provide data **subject to independent verification** by Risk Management. Deviations would be noted and referred to Internal Audit, who would escalate it to the Board. The Board in an exchange is required to provide minutes of all communication to the Regulator, so this became an in-built check and balance.

Step 2:

Each department was asked to provide quantitative assessments of incidence, severity (probability values in both cases) and assessments of loss. These were both point and interval estimates, hence leading to precision. The KRI itself was decided upon with the department in joint consultation with Risk Management and Internal Audit.

[7] A Risk register plots the impact of a given risk over of its probability. It is a scatterplot used as risk management tool and to fulfill regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures.

Step 3:

A mock exercise was first conducted exchange-wide and clearing house-wide. Each team was encouraged to conduct it several times at no penalty till they could get every doubt about the methodology cleared. It was observed that the KRIs altered and the focus of each department became sharper with each iteration. **KRIs, in almost all cases, were combinations of operational risk and another risk type such as market or counterparty credit. This is peculiar to an exchange and clearing house's operation as they basically are large Operating Systems with Market and Credit elements.**

Step 4:

Finally, a pilot exercise was conducted under the joint supervision of Internal Audit and Risk Management. Data was collated and compiled by Risk Management.

Step 5:

Risk Management in an exchange and clearing house routinely conduct multiple stress tests and scenario analyses on a very regular basis. Hence there is always a rich "library" of stress factors and scenarios available. Risk Management, in the presence (with signoff) of Internal Audit, selected a range of such stress factor values and scenarios to be applied to the Expected Loss data in order to calculate the 99.9% OpVAR.

Gap analysis, tabulating results and record keeping

In all cases, for every department, Risk management conducted a KRI assessment exercise independently, with its own assessment of the Incidence and Severity distributions, and Expected Loss values. It was observed that the gaps reduced over time, indicating increasing familiarity of the department with the methodology. There was never any case in over eight quarters of any department having to be reported to the Board for extraordinary deviations (+/- 5%).

The results of each exercise were communicated to the Board Risk Management Committee and the Audit Committee by the CRO and Head of Internal Audit. The minutes of each committee contained the results of each Risk Register exercise and these were communicated to the Regulator each time. Minutes of Board Meetings go into the permanent record and they reside there. The Regulatory audit results improved from Satisfactory to Good and stayed there for eight quarters.

Business Continuity Plans (BCP) and their implementation

The BCP requirement in operational risk

Business Continuity Plans (BCPs) are a regulatory requirement that focuses on the effective recovery and rapid resumption of critical business functions and restoration of information technology infrastructure following operational disruptions. Regulators test whether the BCP is robust and can withstand serious disruptions.

Case study of BCP experience in a major financial institution

In addition to the Risk Register exercise, the exchange and clearing corporation simulated an industry-wide communications breakdown twice every quarter and operated the exchange and clearing from a remote site in each case. Every time the "breakdown" was on a randomly selected weekend and a few parameters were varied that enabled the BCP to be conducted successfully. The following outlines what the regulators observed and appreciated in the BCPs.

Key issues that regulators watch out for in an actual simulation

1. No advance warning beyond 30 minutes, SMS text records to be preserved.
2. Random rotation of staff. No recurrence of same staff at remote site and no patterns in presence or absence of staff.
3. Presence of a majority of counterparties. This is a challenge but can be accomplished by proper communication and explaining the Regulatory requirement to market participants.

Success factors in a BCP from actual experience

1. Reduction of response time from SMS communication to actual operation for each successive BCP cycle till steady state is achieved.
2. Completion of operation for complete working day every time.
3. Completion of clearing and settlement cycles with no delays or defaults.
4. Risk Management: Computation of all parameters and conduct of all Stress Tests and Scenario Analyses as on any other working day.

E-GRC software selection and implementation

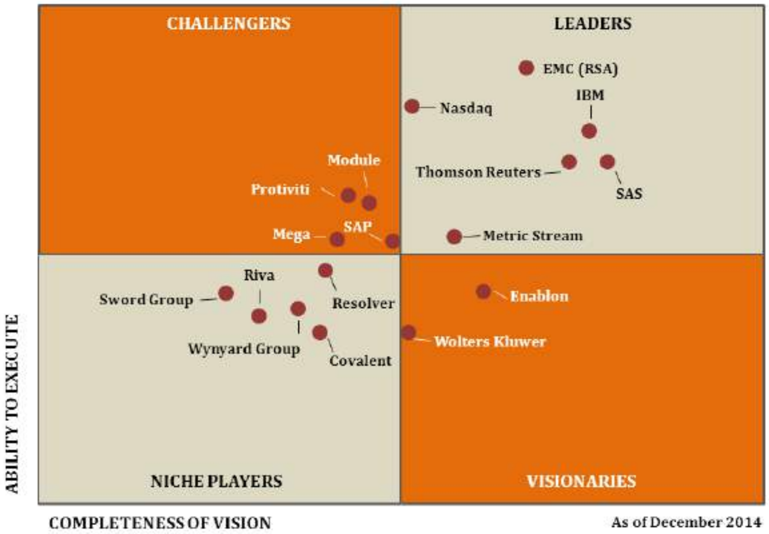
One of the challenges in the running of an operational risk function is the selection and implementation of the appropriate software to conduct enterprise wide risk governance. There are a number of Enterprise Risk Governance and Compliance (E-GRC) software packages available in the market. A brief look at the selection criteria would enable an institution to examine the requirements versus the strengths and weaknesses of the available software.

A useful guide to what is available is contained in the Gartner Magic Quadrant map presented below. Note that this map is an indicator of availability and is largely driven by commitments data. It is prudent to use this as an indicator of availability and the fact that these companies are currently active in the market, hence a small "hedge" against their disappearance at no notice, which is a form of operational risk in itself.

Note that the level of maturity of the operational risk function and closeness to actual 99.9% OpVAR computation should be among the key considerations in E-GRC software selection. Implementation depends clearly on level of support that the software company provides, coupled with the level of maturity of the Tech & Ops function at the bank purchasing the software.

The Gartner map and choices available in the E-GRC software space

The map below indicates that as at December 2014, IBM, SAS and Thomson Reuters were active in the E-GRC space. Given the fact that they are all well capitalized companies, it would perhaps be worthwhile to consider these, as all other things being held constant, the software may meet institutional needs. This is in no way any recommendation for any company in this space but may be used as an indicator of activity from time to time. This quadrant is updated every year.



Gartner Magic Quadrant for Operational Risk Management

Readings:

1. Business Continuity Management Guidelines from Monetary Authority of Singapore (MAS)

CHAPTER 4: IDENTIFICATION TECHNIQUES

Process mapping for operational risk: Mapping by various departments

The Basel Committee on Banking Supervision, Principles for the Sound Management of Operational Risk, June 2011, lists Business Process Mapping as a tool that may be used for identifying and assessing operational risk:

> *"Business process mappings identify the key steps in business processes, activities and organizational 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 prioritize subsequent management action."*

Invoking this concept, we note that process mapping is an integral part of the Risk Register exercise. It is through process mapping that certain elements of "Risk Ownership" are assigned to certain business lines. In Case 3, the mapping was conducted as follows:

Cross section of the Risk Map

Stage 1: Inputs

Level	Example	Risk Ownership
Identification of high level process	Clearing and Settlement risks	Head of Clearing and Settlement
Sub-process/task	Settlement Confirmation risks	Settlement Manager/ Head of Clearing and Settlement

In both cases, one must ascertain:

1. Whether the process is documented?
2. Whether the process is manual/system-based?
3. Whether the process is line/independent?
4. What is the frequency?
5. What is the severity?
6. What are the corresponding processes and sub-process risk controls /mitigants (general/specific)? It was noted during this exercise that specific risks (e.g. fat finger errors), in many cases, can be mapped to multiple categories.
7. This process was repeated across all functions, business lines and units for the exchange and clearing corporation.

Stage 2: Outputs from RCSA

The Risk Register exercise yielded two levels of output:

Output Risk Dashboard:

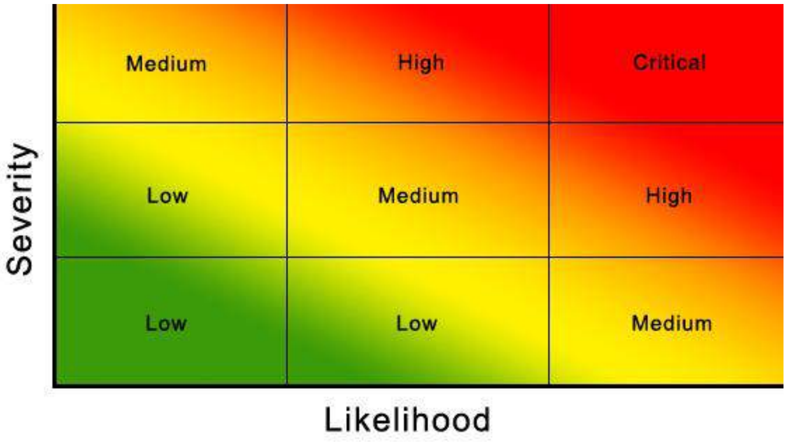
A dashboard outlining each specific risk for each business

A Heat Map:

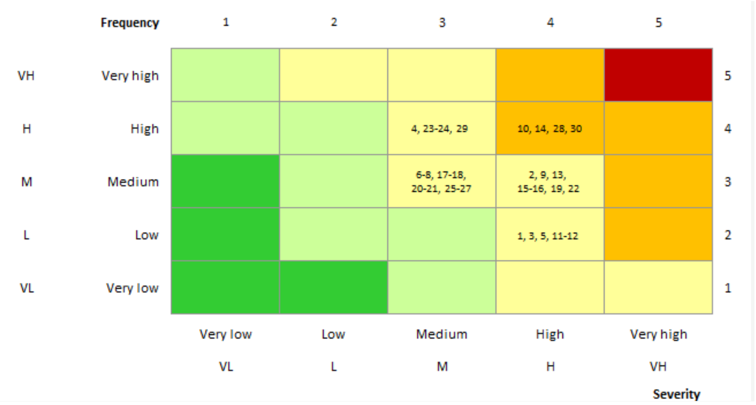
Indicates expected frequency and severity of each risk incidence for each business

Heat Maps:

- Heat maps are a way of representing the resulting qualitative and quantitative evaluations of the probability of risk occurrence and the impact on the organisation in the event that a particular risk is experienced.
- The development of an effective heat map has several critical elements – a common understanding of the risk appetite of the company, the level of impact that would be material to the company, and a common language for assigning probabilities and potential impacts.
- The heat map has two axes: an expected frequency axis and an expected severity axis.
- The bottom left part of the map is a "green light" or low levels of both and the top right part of the map is a "red light" or high levels of both, with amber in between.



The 5x5 heat map diagram below provides an illustration of how organizations can map probability ranges to common qualitative characterizations of risk event likelihood, and a ranking scheme for potential impacts. They can also rank impacts on the basis of what is material in financial terms, or in relation to the achievement of strategic objectives. In this example, risks are prioritized using a simple multiplication formula. A stylized Frequency-Severity Heat Map is presented below.



	Frequency	1	2	3	4	5	
VH	Very high						5
H	High			4, 23-24, 29	10, 14, 28, 30		4
M	Medium			6-8, 17-18, 20-21, 25-27	2, 9, 13, 15-16, 19, 22		3
L	Low				1, 3, 5, 11-12		2
VL	Very low						1
		Very low	Low	Medium	High	Very high	
		VL	L	M	H	VH	
						Severity	

The objective of risk controls is to bring the Heat Map into the amber or green for as many businesses as possible. The progress towards green is the indicator for the effectiveness of the controls.

Training non-Risk departments to identify their KRIs – Case 3

Firstly, all departments were given a primer on Risk Management developed by the CRO's office. The primer explained and distinguished between the various types of risk, with an emphasis on operational risk. They were informally quizzed on the primer in repeated sessions till they achieved a minimum cutoff level of competence in operational risk. The second stage was a session on how to identify KRIs mapping on to various risks within the purview of the particular business unit, and within operational risk, how to identify specific risks.

Care was taken to make the exercise non-threatening. The business units were assured that no penalties would be imposed if a business unit correctly assessed itself as susceptible at a "red light" level to a risk, but alternately their incorrect assessment would be escalated.

For the first exercise, a number of dry runs with inputs from Risk Management and Internal Audit were conducted. It was noticed that the assessments of the business lines began to converge to that of Risk Management and Internal Audit. Finally, when there was a consensus that all the business lines had understood the exercise, it was conducted officially with no guidance.

An advantage of clear two-way communication from the outset was that there were no surprises. Over a two year period, multiple such exercises were conducted and not once was there need for any escalation. The KRIs and their heat maps were duly developed and extensively used, and proved to be a very strong aid in risk mitigation decision making.

Examples: mapping processes, assessing risks, developing KRIs – Case 3

Mapping processes and assessing risks:

Process mapping in all cases started with assignment of risk and intensive contact with risk owners. Each risk owner (roughly a business line head – Ops, Clearing, Settlement, Finance, HR, etc.) first offered a qualitative risk assessment of their particular area's vulnerability. These assessments were then taken to the next level of granularity by their now providing details on typical risk events.

Event analysis:

At this point, the risk assessment ceased to be purely qualitative and each event's impact was translated into expected frequency of incidence, and expected severity of incidence in terms of financial impact.

Developing a KRI:

For each business line, each KRI would imply a positioning on a heat map. Each KRI, therefore, would be unique for each business line, even though it could appear in different business lines. Hence a "fat finger error" specific risk proved to be a different KRI for Confirmation than it was for Surveillance. The process of assigning KRIs was through a combination of Workshops for the identification of risks and Questionnaires from Risk Management and Internal Audit designed to ascertain levels of controls that either exist or need to exist for the business line. Taken together, both the Workshop and Questionnaire help the business line clearly identify its KRIs.

Operational risk scorecards

The organization’s operational risk scorecards are based on Output Risk. It is typically exhaustive and derived from the RCSA. The sources are detailed versus the business units, and their “heat rating” is in the body of the scorecard. It provides a ready reckoner to the management and the Board of the institution about the operational risk status at a point in time.

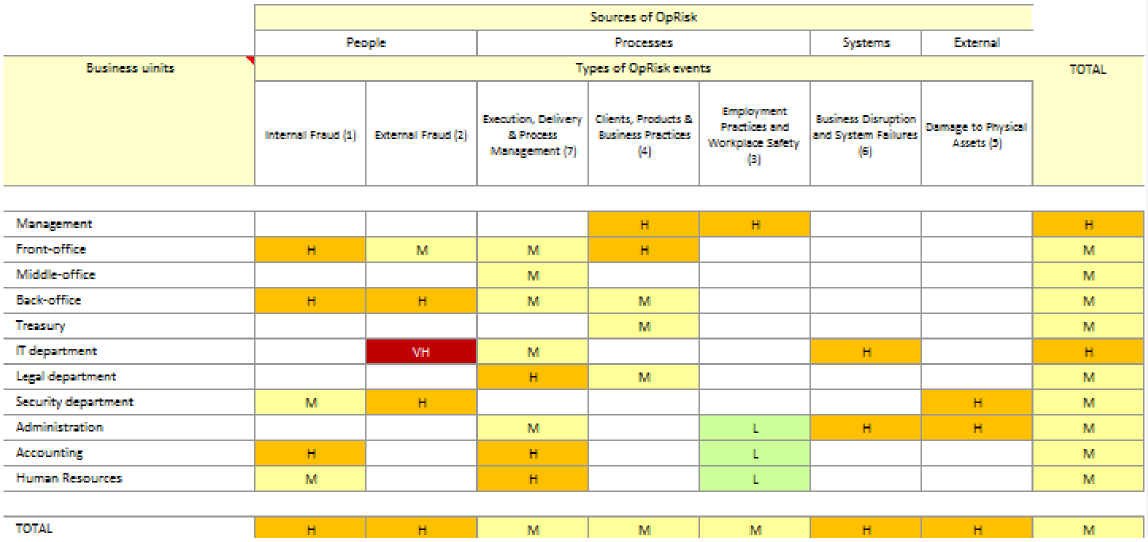
Purpose:

Ready reckoner for the Ops Risk status at any point in time

An operational risk scorecard is a report that shows the operational risk profile of a company or parts of that company, with the help of appropriate scores. This scorecard must achieve several goals:

- Reflect the level of operational risk: this is the primary goal that gives the op risk scorecard its name. The level of risk is determined via an assessment.
- Explain from where in the organization the operational risk comes: the scorecard should reveal what the op risk scores are related to, that is, to which part of the organization, in connection to which products or business lines, which organizational units and which locations of the company.
- Present what the causes of operational risk are: only when the causes of op risk are presented in the scorecard do people understand how the level of op risk is determined, why it is at the level at which it is reported in the scorecard and how it can be reduced.
- Reflect the operational quality: the level of risk in an organization depends on its operational quality, which includes the quality of the control environment. If the operational quality is low, the organization will face a higher risk of losses.
- Focus management attention: the scorecard should not only give a status of the op risk and quality level, but also encourage management to undertake actions to mitigate the risk via quality improvements. Therefore, the scorecard must relate the levels of op risk and quality to each other so management can set priorities for their actions.

A stylized organizational operational risk scorecard is presented in the figure below.



	Sources of OpRisk							
	People		Processes			Systems	External	
Business uinits	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

CHAPTER 6: MEASUREMENT AND REPORTING

The Advanced Measurement Approach

Picking up from the BI, TSA and ASA of Basel II, the next stage is the Advanced Measurement Approach (AMA). Originally, the AMA was open-ended; but as of this point in time, it has clearly evolved into a finite family of techniques with clear protocols for data collection, modeling and performance. This section describes the AMA in depth and in terms of what is expected from banks going forward.

Some math fundamentals

We begin by highlighting a key concept: Gaussian Copulas, which are extensively used in the AMA.

A Gaussian Copula is a distribution over the unit cube $[0,1]^d$. It is constructed from a multi-variate normal distribution over $\mathbb{R}^d$ by using the probability integral transform.

For a given correlation matrix $R \in \mathbb{R}^{d\times d}$, the Gaussian copula with parameter matrix R can be written as:

$$C_R^{\text{Gauss}}(u) = \Phi_R\left(\Phi^{-1}(u_1), \dots, \Phi^{-1}(u_d)\right),$$

where Φ^{-1} is the inverse cumulative distribution function of a standard normal and Φ_R is the joint cumulative distribution function of a multivariate normal distribution with mean vector zero and covariance matrix equal to the correlation matrix R.

The density can be written as:

$$c_R^{\text{Gauss}}(u) = \frac{1}{\sqrt{\det R}} \exp\left(-\frac{1}{2}\begin{pmatrix}\Phi^{-1}(u_1)\\ \vdots \\ \Phi^{-1}(u_d)\end{pmatrix}^T \cdot \left(R^{-1} - \mathbf{I}\right) \cdot \begin{pmatrix}\Phi^{-1}(u_1)\\ \vdots \\ \Phi^{-1}(u_d)\end{pmatrix}\right),$$

where $\mathbf{I}$ is the identity matrix.

The application of Copulas in AMA is a transformation of a correlation structure to include:

1. Transformations of relationships
2. Cumulation or addition of Expected and Unexpected Loss Distributions
3. The inclusion of KRIs in Normalized (restricted to being bounded between 0 and 1)

Let us examine the AMA approach given this background.

The goal of AMA

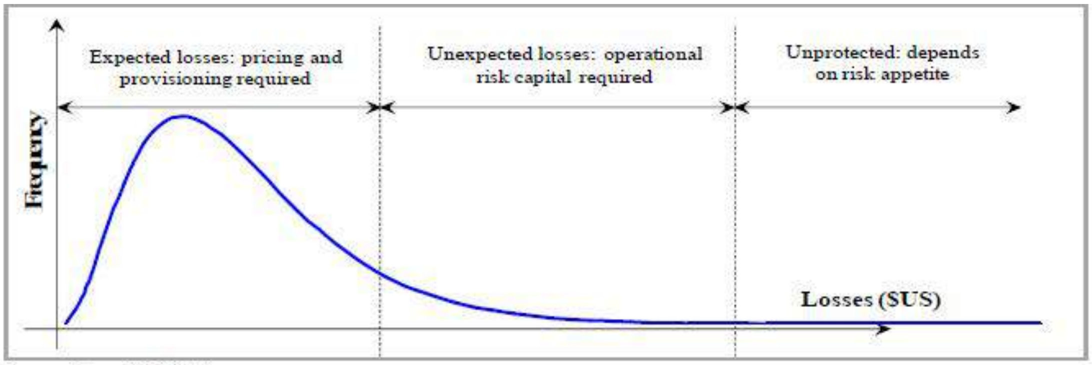
The goal of AMA is to derive a capital charge such that all extreme losses up to the 99.9th percentile are taken into account.

Capital Charge under AMA = Expected Loss + Unexpected Loss

Amount of loss

1. Expected Loss, in the case of operational risk, is the empirical distribution of the extreme values of a Normal distribution. The mean of the extreme values is the average Expected Loss, and its upper bound is the 99.9% Value at Risk or OpVAR.

2. **The stochastic component of OpVAR is the Unexpected Loss provision.**
3. Stress Losses are above and beyond 99.9% OpVAR and are not part of the AMA capital charge. The entire exercise is in order to reach this goal.



Source: Cruz (2002:211)

Historical data

Since we are concerned with the empirical distribution of extreme values, we need to collect historical data, and since its upper bound is the 99.9% percentile, we need a very large number of data points. Since 10,000 data points will be needed to reach a 99.9% confidence level, we need to collect data from all sources—internal and external.

Characteristics:

1. The data should capture potentially severe tail loss events at one year holding period and a 99.9th percentile confidence interval. Hence the Risk model and its validations should be based on data history of not less than 3 years (at initial recognition) and over 5 years (in next calculations).
2. It should be consistent with scope of BCBS Op Risk definition and loss event types.
3. It should be sufficiently granular to capture the major drivers of Op Risk affecting the shape of the tail of the loss estimates.
4. Correlations across individual operational risk estimates should be recognized by the regulators as sound and implemented with integrity.
5. Data, in this case, should include the use of internal data, relevant external data, scenario analysis, RCSA and KRIs, and must be credible, transparent, well-documented and verifiable.

The Loss data that has to be collected comprise **Op Risk losses** –defined as negative and quantifiable impacts on P&L due to an Op Risk event. This includes **Single losses** – a total amount of all Op Risk losses pertained to a single loss event, **Grouped losses** – Op Risk losses with the same underlying cause that arise from single events within a Business Line and between Business Lines and finally, **Root loss** – the initial single event without which none of the grouped related losses would have occurred.

For risk calculation and reporting purpose grouped losses have to be considered and recorded as a single root event. The points in time for with which data needs to be collected, for each loss, are:

1. Date of Occurrence
2. Date of Discovery
3. Date of Reporting

4. Date of Accounting
5. Date of Settlement

The business and control environment

The qualifying standards for any bank implementing AMA are that:

1. The minimum qualifying criteria used for TSA are met.
2. The bank has an independent full-fledged ORM function.
3. ORM is closely integrated in day-to-day activity.
4. Regular reporting and action taking processes exist and are audited.
5. The bank's ORM practice is documented, reviewed and validated by internal and external audit on a regular basis.

Scenario analysis

According to BCBS, "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 forward looking 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.***

Scenario analysis is a part of AMA quantitative standards for Basel II, which requires that a bank use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events.

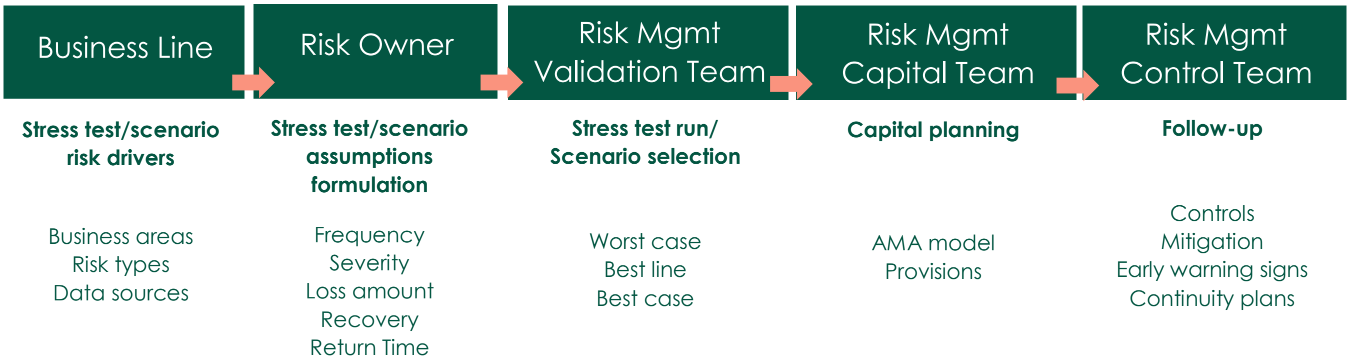
Stress testing

Stress testing is also a forward looking procedure. In many ways parallel to scenario analysis, it is less qualitative and consists of shocking risk drivers to limits and then measuring the impact of these shocks. Consequently, the Scenario Analysis/Stress Testing Framework consists of two parts:

1. The process
2. The procedure (writing the Stress Testing/ Scenario Analysis algorithm)

The stress testing/ scenario analysis process

The role of various teams and sub-teams in Stress testing/Scenario Analysis is illustrated in the following flow diagram:



Steps in the stress testing/ scenario analysis procedure: Writing the algorithm

1. Defining and structuring the stress test/scenario analysis: Describing important risk drivers/external factors and their influence on the stress test/scenario analysis. These risk drivers/external factors form the risk influence fields.
2. Identifying major descriptors for each risk influence field and making assumptions about their future trends.
3. Checking the consistency of possible combinations of alternative assumptions regarding the risk influence fields and identifying assumption bundles.
4. Combining assumptions with the trend assumptions regarding the risk influence fields, resulting in a stress test/scenario analysis for each field.
5. Assessing the impact of the stress tests/ scenario analysis on P&L.
6. Identifying strategies that could promote or impede the developments described in the stress tests/scenario analysis.

Combining the building blocks in AMA

Calculating the capital charge for 99.9% OpVAR via the IMA

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

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

$$PE_{ij} = \frac{\sum EI_{ij} \Big|_{LE_{ij}>0}}{\sum EI_{ij}}$$

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

The Internal Measurement Approach (IMA) is based on linear proxy between expected loss (EL) & unexpected loss (UL).

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:

1. Number of transactions
2. Total turnover of operations
3. Average volume of transactions
4. Gross income of operations

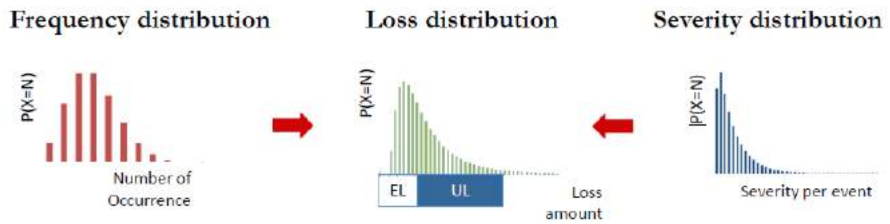
A stylized example of the IMA

Business Line	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 (OPVAR 99.9%)						**73.7**

Calculating the Capital Charge for 99.9% OPVAR via the LDA

1. Loss Distribution Approach (LDA) estimates for each business line or event type are derived from the likely distribution of Op Risk losses over a certain period of time (1 year) at required confidence level (99.9%).
2. LDA measures UL directly with the loss distribution derived from assumptions of loss frequency and severity distributions and correlations between loss events. The LAMA uses the OpVAR.

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



Reporting operational risks

There are various reports that have to be prepared and disseminated for the operational risk function.

1. Reports on Risk Indicators have to be collected by Risk Owners and submitted to Internal Audit and Risk management on a Monthly, Quarterly and Annual basis.
2. Reports on Retrospective Indicators, Regression Forecasts and Thresholds check have to be submitted by Risk Management to Internal Audit and the Board Risk and Audit Committees on a Quarterly basis and the Operational Risk Management Committee on a Monthly and Quarterly basis.
3. Reports on Business plan Indicators / Thresholds Check have to be presented by Risk Management and Internal Audit to the Board Risk and Audit Committees on a Quarterly basis and the Operational Risk Management Committee on a Monthly and Quarterly basis.
4. Reports on Peers Comparison / Thresholds Check have to be presented by Risk Management and Internal Audit to the Board Risk and Audit Committees on a Quarterly basis.

CHAPTER 8: BEST PRACTICES AND CONCLUSIONS

Managing extreme risks: technical issues and distributions

The most convenient manner in which to imbibe best practices is to perform one illustrative best practice run. Here, we compute a 99.9% OpVar by invoking the Poisson distribution, which is a BCBS approved best practice.

The objective is to build an internal model that could lead to a direct calculation of the amount of expected and unexpected loss, with 99.9% Interval of Confidence, over a one year time period.

The first step is to assess the probability of a failure. In order to do so, we ask:

How many operational failures do we expect to occur in the next 12 months?

OR

Over how many years do we expect an operational failure to occur?

We can then use this number as the parameter λ for a Poisson distribution.

The Poisson distribution

- A probability distribution that often used to model tail events[8].
- It is a mathematical rule that assigns probabilities to the number of occurrences of a certain event within a certain time period.
- The Poisson distribution has only one parameter λ representing both mean and variance.

For example, if we expect a fraud to occur once in the next 5 years and if these events are Poisson distributed, then the parameter of the distribution will be 0.2 (i.e. 1/5) and the probability of k frauds to occur in 1 year will be:

$$P(\#Failures = k) = e^{-\lambda}\frac{\lambda^{k}}{k!}$$

– where λ=.2

If k = 1, and λ=0.2, then the Probability (or Likelihood) is approximately at 0.5.

Assessing severity of an operational loss

Next, we ask the question:

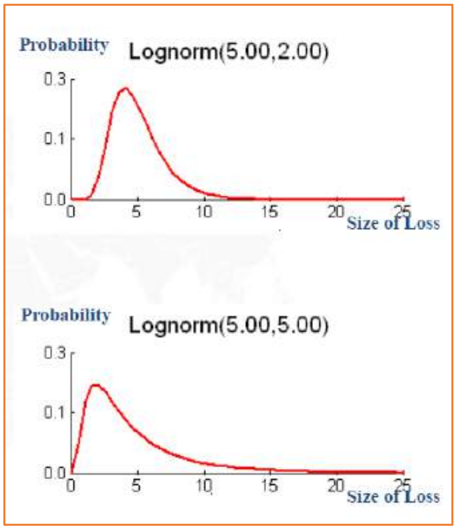
Should a failure happen, what is the expected operational loss?

If we set the confidence level at 99.9%, we ask the same question as follows: How much more can we lose, say, 99.9% of the time? (so that we will lose more only 1 in 10000 times).

For certain distributions (for example, normal and lognormal), this is all we need to fully identify the distribution.

[8] Events that are the exception rather than the rule

The Lognormal distribution has two parameters representing mean and standard deviation respectively. To translate this into monetary terms, make loss assumptions.



For example:

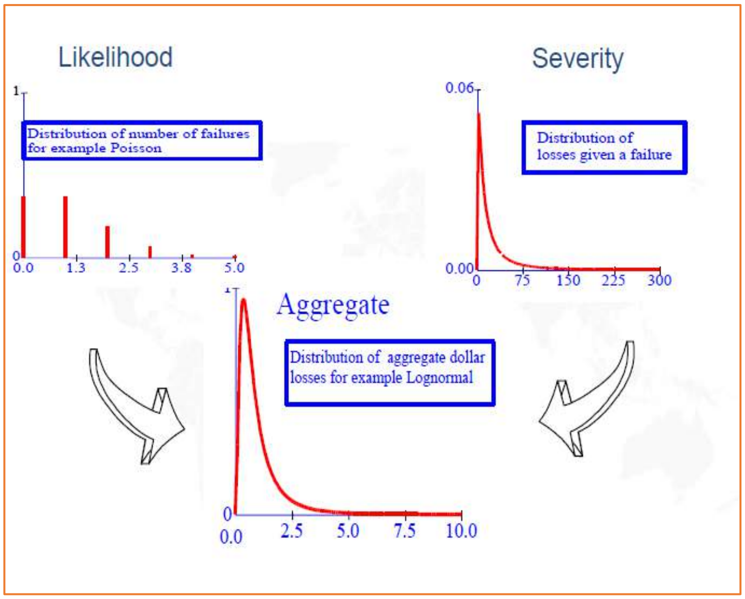
Assume that a settlement mistake will cost on average €50,000 with a standard deviation of €200,000. If the losses are distributed according to a lognormal distribution, this means that 99.9% of the time, the loss will not exceed €650,000 or 3 standard deviations plus the mean.

The probability of losing exactly €x will be given by the following formula.

$$P(x) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{(\ln x - \mu)^2}{2\sigma^2}}$$

where μ=50.000 and σ =200.000

Now, we cumulate (if not exactly add up) the Likelihood and Severity distributions.


Likelihood
1
0
Distribution of number of failures for example Poisson
0.0
1.3
2.5
3.8
5.0
Severity
0.06
0.00
Distribution of losses given a failure
0
75
150
225
300
Aggregate
1
0
Distribution of aggregate dollar losses for example Lognormal
0.0
2.5
5.0
7.5
10.0

If the γ value of the Copula[9] is set to be 0.5, then the cumulation of the two distributions gives us OpVAR at 99.9%

= Likelihood x Severity x γ

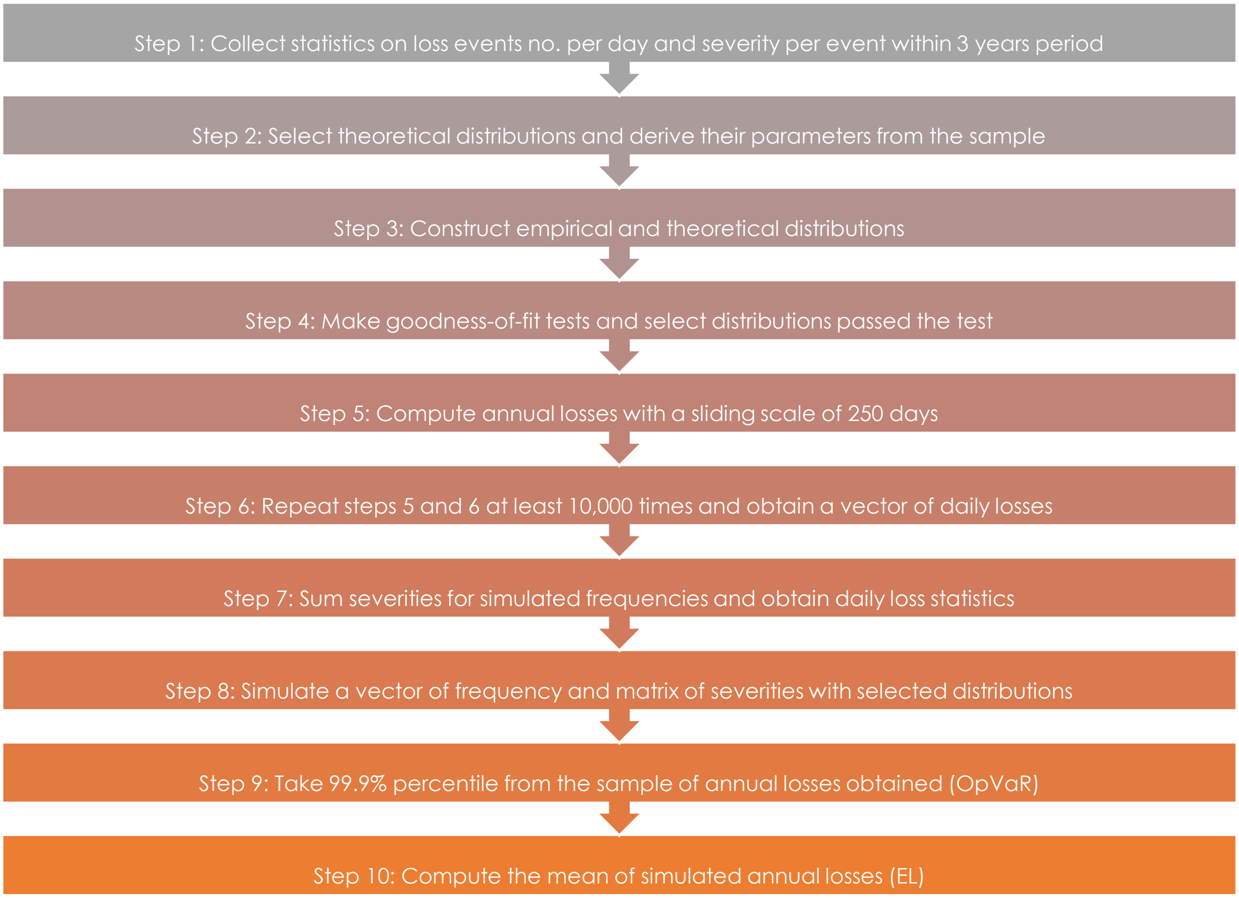
i.e. OpVAR = 0.5 x 650,000 x 0.5

= €1,625,000

As the adjacent graph shows, it corresponds to the central (mean or median value) of the cumulated distribution.

[9] In probability theory and statistics, a copula is a multivariate probability distribution for which the marginal probability distribution of each variable is uniform. Copulas are used to describe the dependence between random variables. In risk portfolio management, copulas are used to perform stress-tests and robustness checks that are especially important during "downside/crisis/panic regimes" where extreme downside events may occur (e.g., the global financial crisis of 2007–2008).

The following steps show the operational best practice in the simulation of Operational Losses via algorithms for banks:



Step 1: Collect statistics on loss events no. per day and severity per event within 3 years period

Step 2: Select theoretical distributions and derive their parameters from the sample

Step 3: Construct empirical and theoretical distributions

Step 4: Make goodness-of-fit tests and select distributions passed the test

Step 5: Compute annual losses with a sliding scale of 250 days

Step 6: Repeat steps 5 and 6 at least 10,000 times and obtain a vector of daily losses

Step 7: Sum severities for simulated frequencies and obtain daily loss statistics

Step 8: Simulate a vector of frequency and matrix of severities with selected distributions

Step 9: Take 99.9% percentile from the sample of annual losses obtained (OpVaR)

Step 10: Compute the mean of simulated annual losses (EL)

Validation of advanced measurement models

Note that Step 4 in the 10 steps above is a validation step. AMA models have some validation methodologies that are tested and preferable. This is applicable to the Loss Distribution Approach (LDA).

Likelihood Distributions	
Currently allowed Likelihood Distributions	**Their Validation Tests**
Poisson	χ2-test
Negative	

Severity Distributions	
Currently allowed Likelihood Distributions	**Their Validation Tests**
Lognormal	Q-Q plot
Pareto	K-S test
Weibull	