CONFIDENTIAL – NOT FOR PUBLIC DISTRIBUTION
CENTRAL BANK USE ONLY!

Underlying Concepts for Building a Sound AMA Framework

Financial Stability Institute
Basel, Switzerland
October 24-26, 2006

Ali Samad-Khan
President, OpRisk Advisory
Stamford, CT
www.opriskadvisory.com

OpRisk Advisory – Company Profile

OpRisk Advisory

> opriskadvisory.com

OpRisk Advisory is the world's leading operational risk management consulting firm. We provide the full range of services to help our clients develop highly-efficient, cost-effective operational risk management programs that meet or exceed industry best practices and satisfy the highest level of Basel II compliance.

Advisory & Consulting Services

We have advised many of the world's largest banks, insurance companies, energy companies and regulators on the full range of operational risk measurement and management issues. As a result, we are able to share many valuable lessons – lessons learned the hard way – about what works, what doesn't work and how it all fits together.

VaR Modeling

Modeling operational risk is far more challenging than modeling market or credit risk. For example, modeling operational risk requires both internal and external loss data, but internal data is insufficient and external data is not directly relevant (e.g., requires scaling for size, controls, data capture). Without addressing these two issues objectively and scientifically, it is difficult to see how the results could be meaningful. We have significant experience in addressing these types of issues and can offer you practical, theoretically valid solutions.

Training & Education

Through short workshops and management seminars we help shed light on many issues that are causing confusion throughout the industry.

France
12-14
Rond Point des Champs Elysées
75008 Paris, France
T: +33 (0) 1 53 53 16 07
F: +33 (0) 1 53 53 14 00

Malaysia
Level 40, Tower 2
Petronas Twin Towers
50088 Kuala Lumpur, Malaysia
T: +603 2168 4490
F: +603 2168 4201

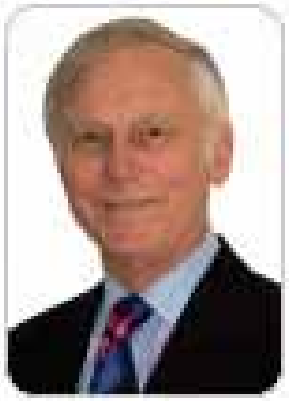
Singapore
80 Raffles Place
UOB Plaza 1, Level 36
Singapore 048624
T: +65 6248 4702
F: +65 6248 4531

Switzerland
Seefeldstrasse 69
Zurich, 8008
Switzerland
T: +41 (0) 43 488 37 69
F: +41 (0) 43 488 35 00

USA
263 Tresser Boulevard
9th Floor
Stamford, CT 06901
T: +1 203 564 1990
F: +1 203 564 1402

OpRisk Advisory – Management Team

Ali Samad-Khan
President



David Lawrence
Executive Director

Stéphane Le Blévec
Principal

Armin D. Rheinbay
Principal

CONFIDENTIALITY

Our clients' industries are extremely competitive. The confidentiality of companies' plans and data is obviously critical.

Similarly, financial risk management consulting is a competitive business. We view our approaches and insights as proprietary and therefore look to our clients to protect OpRisk Advisory's interests in our presentations, methodologies and analytical techniques. Under no circumstances should this material be shared with anyone third party without the prior written consent of OpRisk Advisory.

Agenda

I. Introduction
II. What is Risk?
III. What is Risk Assessment?
IV. What are Risks & Controls?
V. What is Modern ORM?
VI. Summary & Conclusions
VII. Questions & Answers

INTRODUCTION

The importance of a sound operational risk management (ORM) Framework.

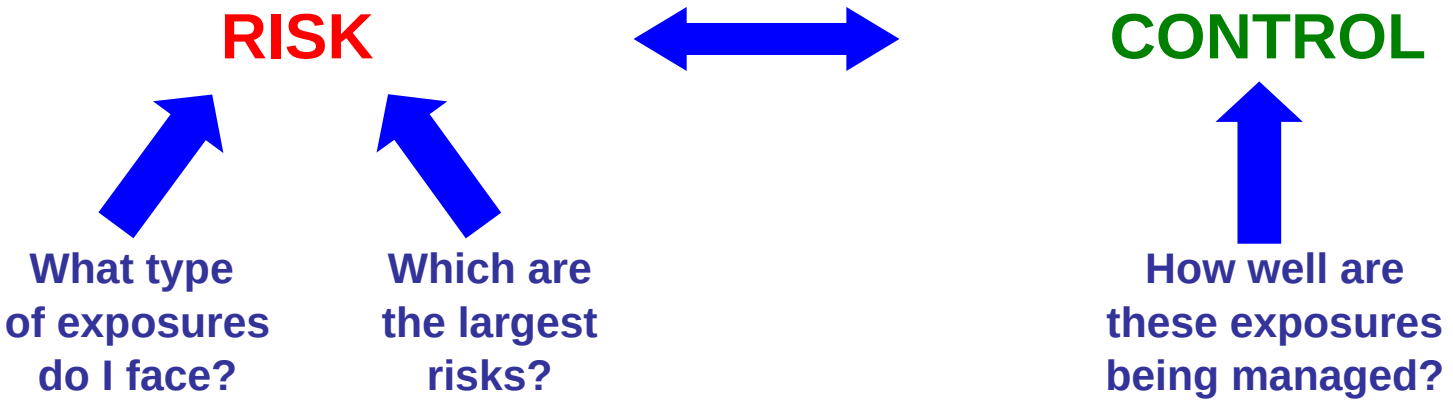
- Good ORM is independent of Basel II compliance.
- The fundamental concepts underlying a sound ORM framework are the same for the AMA, the TSA and even the BIA.
- Banks that have implemented sound ORM frameworks will (almost) automatically comply with all Basel II requirements.
- However, just following the rules will not necessarily guarantee compliance, nor will doing so necessarily add any value.
  - The “use test” will reveal whether some banks are following the letter, but not the spirit, of Basel II.

Risk management means managing the risk reward relationship. When entering a new business one must consider reward in the context of risk inherent to the new business.

Once an organization has invested in a business, risk management involves managing the risk-control relationship in the context of cost-benefit analysis.

RISK  **CONTROL**

Operational risk management is the process of optimizing the risk-control relationship in the context of cost-benefit analysis.



So why are banks having such a difficult time establishing viable ORM programs?

- Many banks don't focus on their major risks, instead they focus on the risks they know about.
- The known risk are typically the smaller risks; whereas the lesser known risks are typically the larger risks.
- As a result most banks are over-controlled in areas where they have the least risk and under-controlled in areas where they have the greatest risk.
- The underlying source of confusion is a misunderstanding about the true meaning of the words **risk, risks** and **controls.**
- The Basel II documents do not explicitly define these terms.

The Basel II regulations do not explain what is meant by the term risk. This is perhaps the greatest source of confusion across the industry.

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

- Basel Committee on Banking Supervision

WHAT IS RISK?

What is risk?

- A kind of unpleasant or undesirable incident, such as a fraud, a market downturn or a system failure.
- A measure which can be calculated as the product of likelihood and impact.
- A measure of the level of exposure at a specified confidence level in excess of the mean.

The best way to illustrate risk is through an example.

Security A	Guaranteed return of 10%
Security B	50% probability of a 0% gain 50% probability of a 20% gain
Security C	50% probability of a 10% loss 50% probability of a 30% gain

Which investment has the highest expected return?

Which investment has the most risk?

How much risk is there in each investment?

Which security is the best investment?

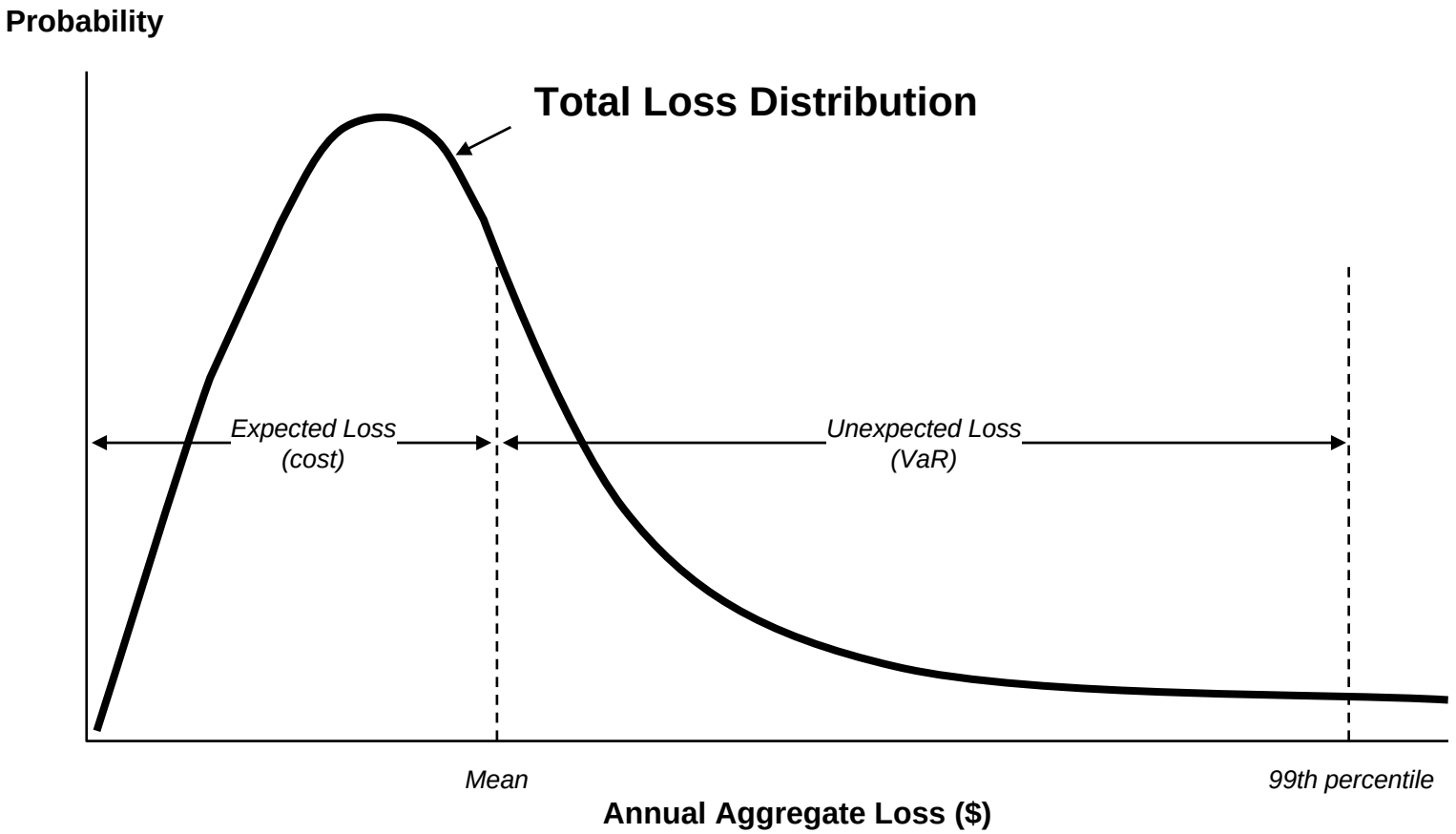
What can we conclude about risk?

- Risk has to do with uncertainty (where there is certainty there is no risk – Security A).
- Risk must be measured at a level of uncertainty (confidence level, e.g., 99%).
- However, it is often possible to rank risks without specifying a confidence level.
  - We know that Security A is less risky than Security B which is less risky than Security C, even without knowing how much risk each investment poses at the 99% level.

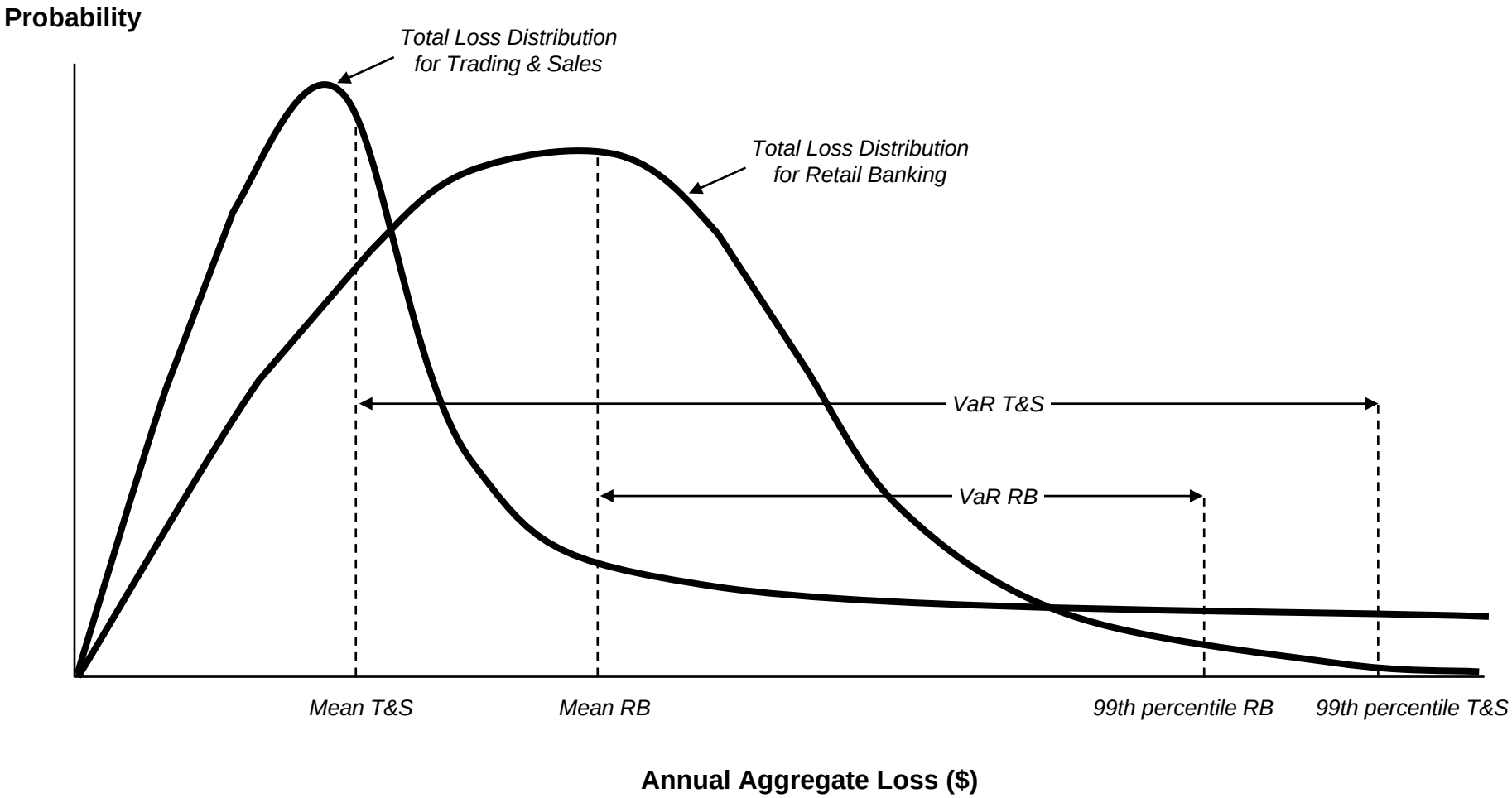
What else do we know about risk?

- Risk is neither inherently good nor bad.
- A risk-neutral person will consider all three investments to be of equal value.
- A risk lover will choose Security C because it offers the higher possible return (30%) among choices with the same expected return (10%) and because risk increases his/her utility.
- Because most people are risk averse, they require more reward for assuming more risk, so will choose Security A. (Equal return with no risk).

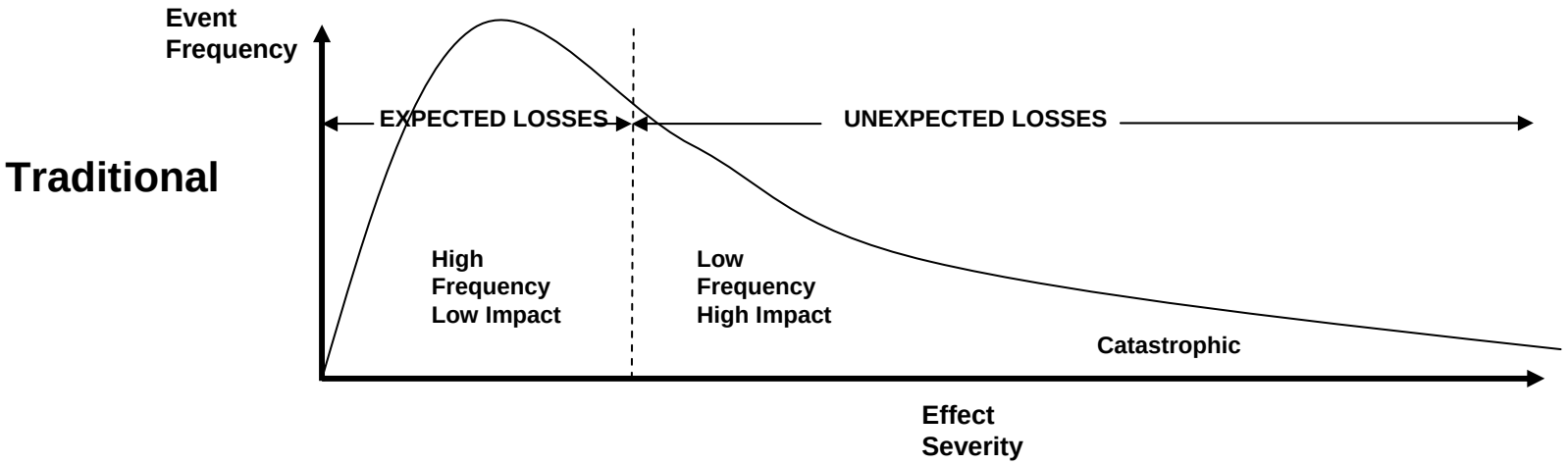
Operational risk is measure of the level of loss exposure at a specified confidence level in excess of the mean.

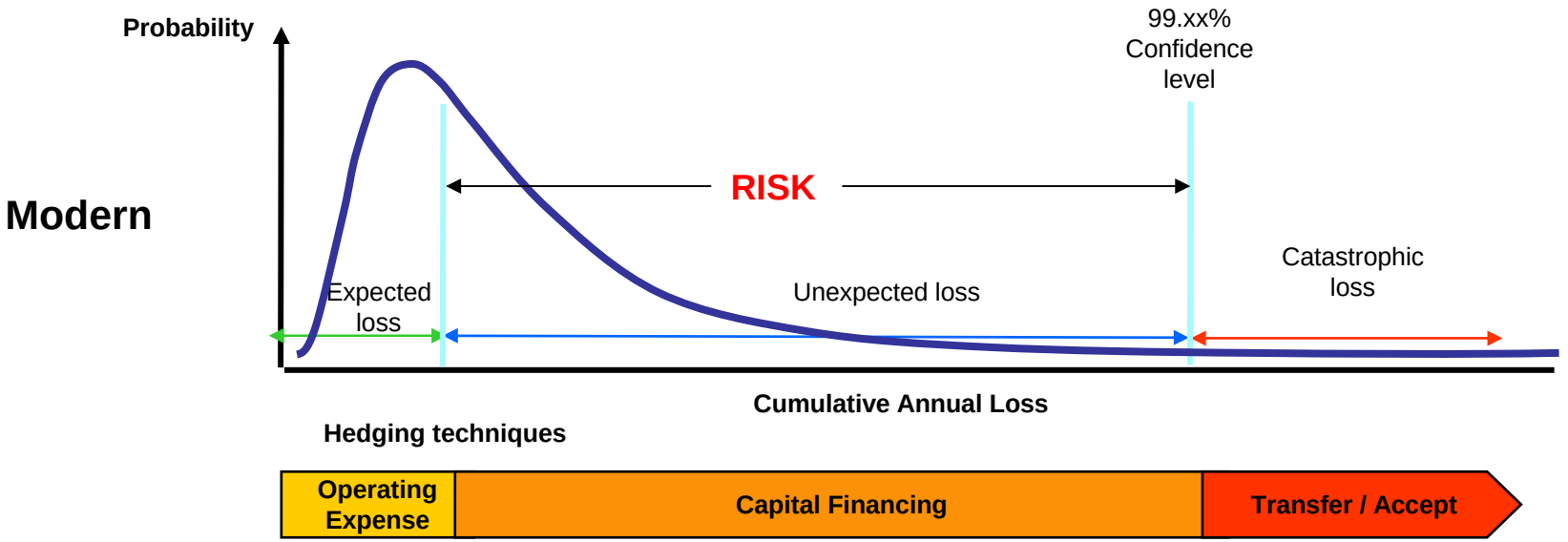


The relationship between the unexpected loss and the expected loss (UL to EL ratio) varies across businesses. A high UL to EL ratio represents high risk (normalized for size).



Many ORM managers still don't realize that the terms expected loss (cost) and unexpected loss (risk) are technical terms which have specific meaning under Basel II.



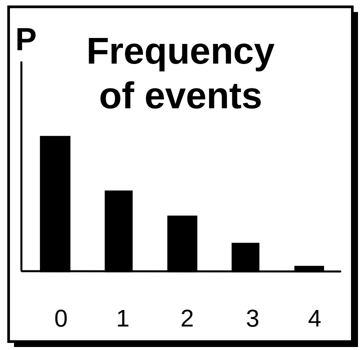


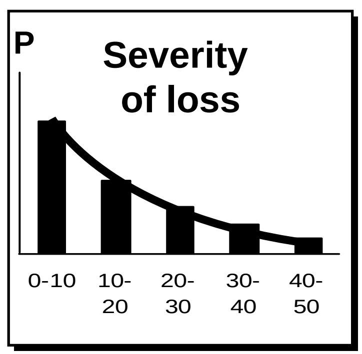
Since operational risk is measured in terms of the aggregate loss, there are two components to operational risk: Frequency and Severity. Unlike in market and credit risk there is no upper limit in operational risk.

INDIVIDUAL LOSS EVENTS | **RISK MATRIX FOR LOSS DATA** | **LOSS DISTRIBUTIONS** | **VAR CALCULATION** | **TOTAL LOSS DISTRIBUTION**

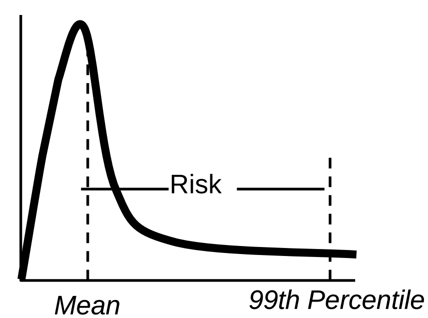
74,712,345
74,603,709
74,457,745
74,345,957
74,344,576
•
•
•
167,245
142,456
123,345
113,342
94,458

		INTERNAL FRAUD	EXTERNAL FRAUD	EMPLOYMENT PRACTICES & WORKPLACE SAFETY	CLIENTS, PRODUCTS & BUSINESS PRACTICES	DAMAGE TO PHYSICAL ASSETS	EXECUTION, DELIVERY & PROCESS MANAGEMENT	BUSINESS DISRUPTION AND SYSTEM FAILURES	TOTAL
Corporate Finance	Number	36	3	25	36	33	150	2	315
	Mean	35,459	52,056	3,456	56,890	56,734	1,246	89,678	44,215
	Standard Deviation	5,694	8,975	3,845	7,890	3,456	245	23,543	6,976
Trading & Sales	Number	50	4	35	50	46	210	3	441
	Mean	53,189	78,084	5,184	85,335	85,101	1,869	134,517	66,322
	Standard Deviation	8,541	13,463	5,768	11,835	5,184	368	35,315	10,464
Retail Banking	Number	45	4	32	45	42	189	3	397
	Mean	47,870	70,276	4,666	76,802	76,591	1,682	121,065	59,690
	Standard Deviation	7,687	12,116	5,191	10,652	4,666	331	31,783	9,417
Commercial Banking	Number	41	3	28	41	37	170	2	357
	Mean	43,083	63,248	4,199	69,121	68,932	1,514	108,959	53,721
	Standard Deviation	6,918	10,905	4,672	9,586	4,199	298	28,605	8,476
Payment & Settlements	Number	37	3	26	37	34	153	2	321
	Mean	38,774	56,923	3,779	62,209	62,039	1,363	98,063	48,349
	Standard Deviation	6,226	9,814	4,205	8,628	3,779	268	25,744	7,628
Agency Services	Number	44	4	31	44	40	184	2	386
	Mean	46,529	68,308	4,535	74,651	74,446	1,635	117,675	58,018
	Standard Deviation	7,472	11,777	5,045	10,353	4,535	321	30,893	9,154
Asset Management	Number	40	3	28	40	36	165	2	347
	Mean	41,876	61,477	4,081	67,186	67,002	1,472	105,908	52,217
	Standard Deviation	6,725	10,599	4,541	9,318	4,081	289	27,804	8,238
Retail Brokerage	Number	48	4	33	48	44	198	3	417
	Mean	50,252	73,773	4,898	80,623	80,402	1,766	127,090	62,660
	Standard Deviation	8069	12719	5449	11182	4898	347	33365	9886
Insurance	Number	43	4	30	43	39	179	2	375
	Mean	45,226	66,395	4,408	72,561	72,362	1,589	114,381	56,394
	Standard Deviation	7,262	11,447	4,904	10,063	4,408	312	30,028	8,897
Total	Number	435	36	302	435	399	1,812	24	3,806
	Mean	45,653	67,021	4,450	73,245	73,044	1,604	115,459	56,926
	Standard Deviation	7,331	11,555	4,950	10,158	4,450	315	30,311	8,981





VaR Calculator e.g., Monte Carlo Simulation Engine



What are inherent risk and residual risk?

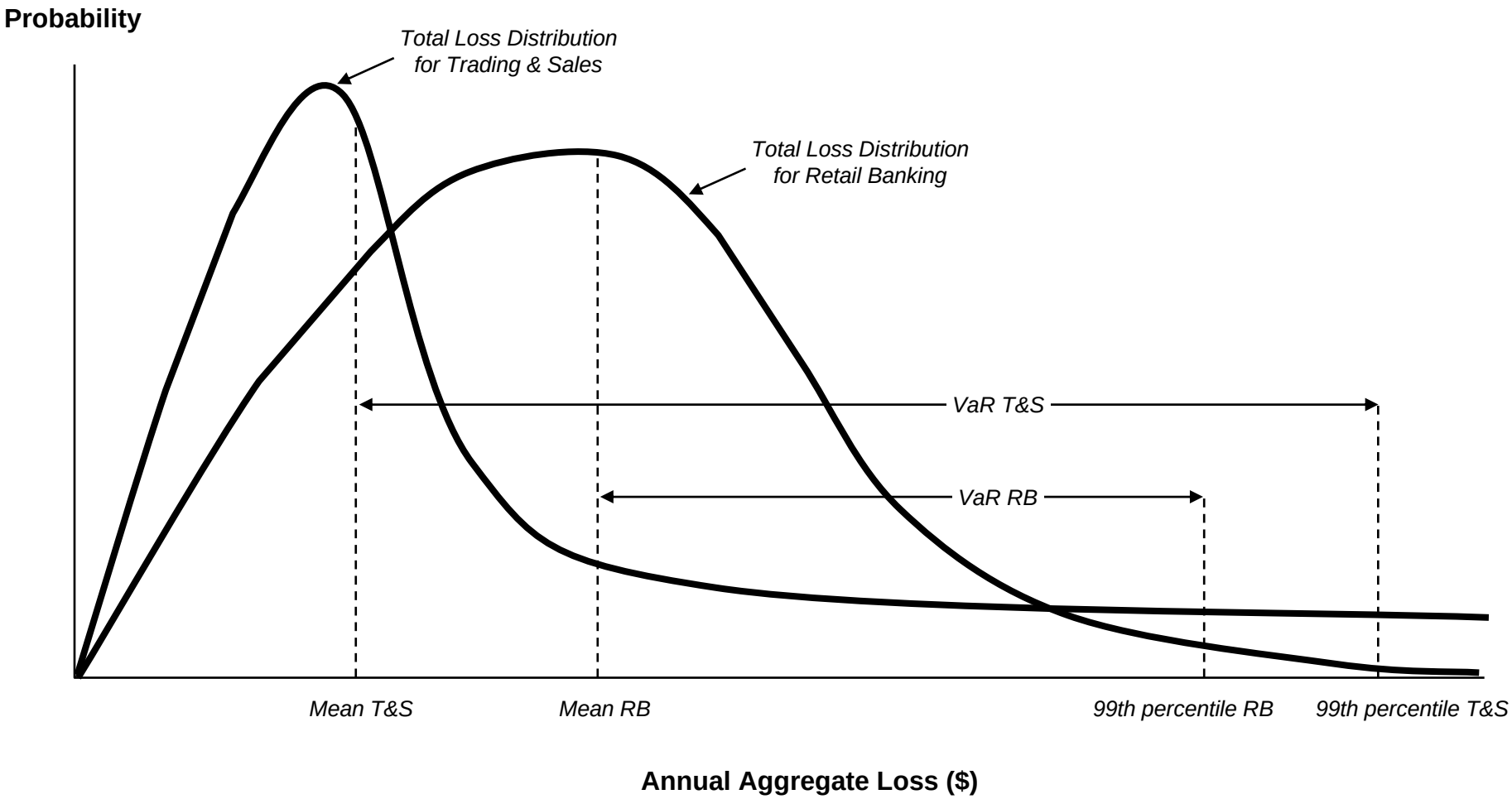
- Is inherent risk the level of risk before controls or in the absence of controls? Is residual risk the level of risk after improving controls?

- Consider an example, if you had $1,000,000 in your bank vault and you had no controls:
    - How much would you expect to lose?
    - How much risk would you have with no controls?
    - How much risk would you have after improving controls?

What are inherent risk and residual risk (continued)?

- The word inherent is defined as unique, permanent or unchangeable.
  - Therefore inherent risk must be the risk that is unique to a particular business or process.
- If the level of inherent risk changes after controls, then by definition that cannot be the level of inherent risk.
- Inherent risk is static. Therefore, the terms inherent and residual risk cannot be used in the same context.

Distributional analysis helps one understand the inherent differences in risk profiles between the different business lines. The relative differences in Inherent risk can be seen when you factor out controls.



WHAT IS RISK ASSESSMENT?

Risk can also be assessed using a likelihood-impact approach. This approach has been well documented by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Risk Assessment

Risk assessment allows an entity to consider how potential events might affect the achievement of objectives. Management assesses events from two perspectives: likelihood and impact.

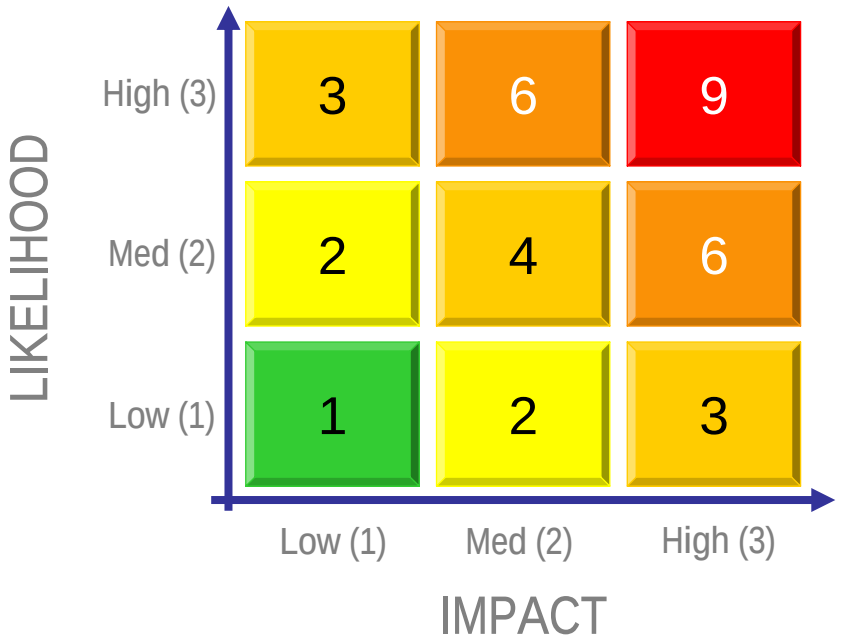
Likelihood represents the possibility that a given event will occur, while impact represents its effect should it occur. Estimates of risk likelihood and impact often are determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates. Internally generated data based on an entity's own experience may reflect less subjective personal bias and provide better results than data from external sources. However, even where internally generated data are a primary input, external data can be useful as a checkpoint or to enhance the analysis. Users must be cautious when using past events to make predictions about the future, as factors influencing events may change over time.

An entity's risk assessment methodology normally comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments either are not practicably available or obtaining or analyzing data are not cost-effective. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques. An entity need not use common assessment techniques across all business units. Rather, the choice of techniques should reflect the need for precision and the culture of the business unit. In any event, the methods used by individual business units should facilitate the entity's assessment of risks across the entity.

Source: COSO

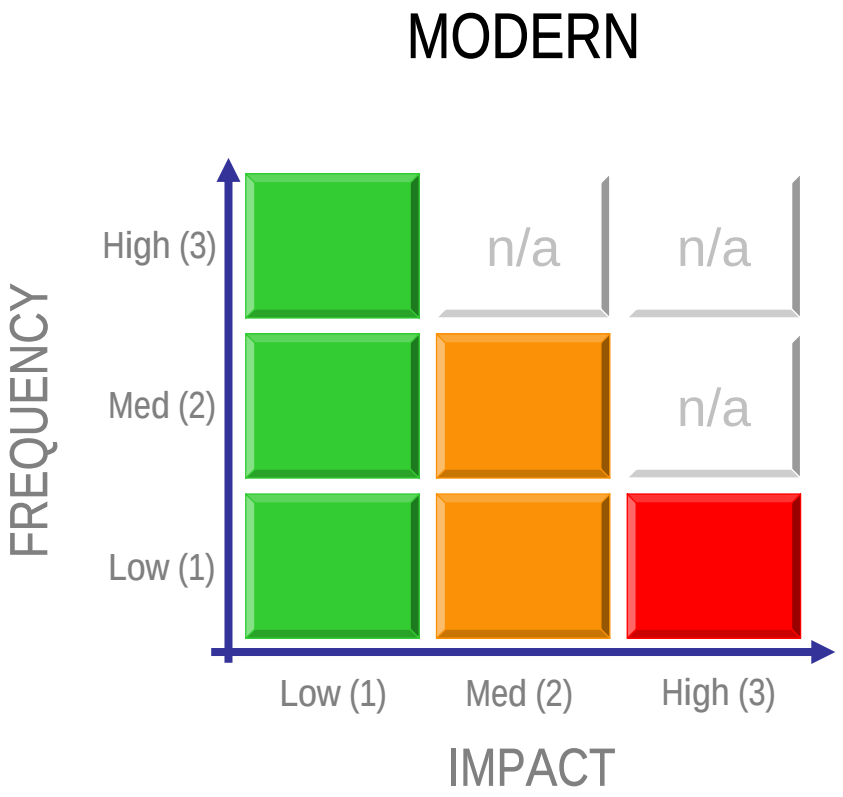
The COSO view of risk assessment is based on the likelihood and impact of a specific incident; the output is probability-weighted impact. The high risk area is in the top right corner of the matrix.

TRADITIONAL



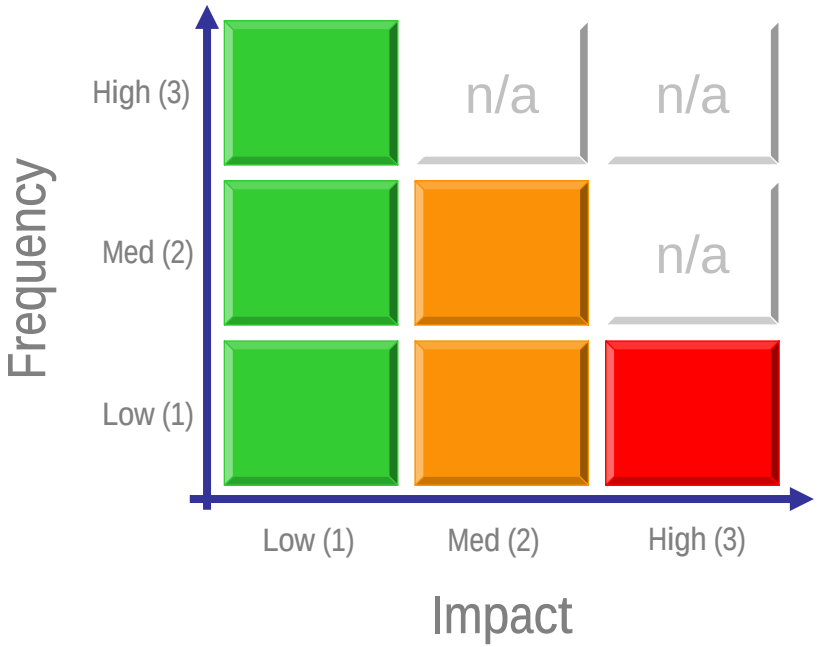
Likelihood x Impact = Risk

Under the risk management industry approach, the high risk area is the bottom right cell in the matrix.

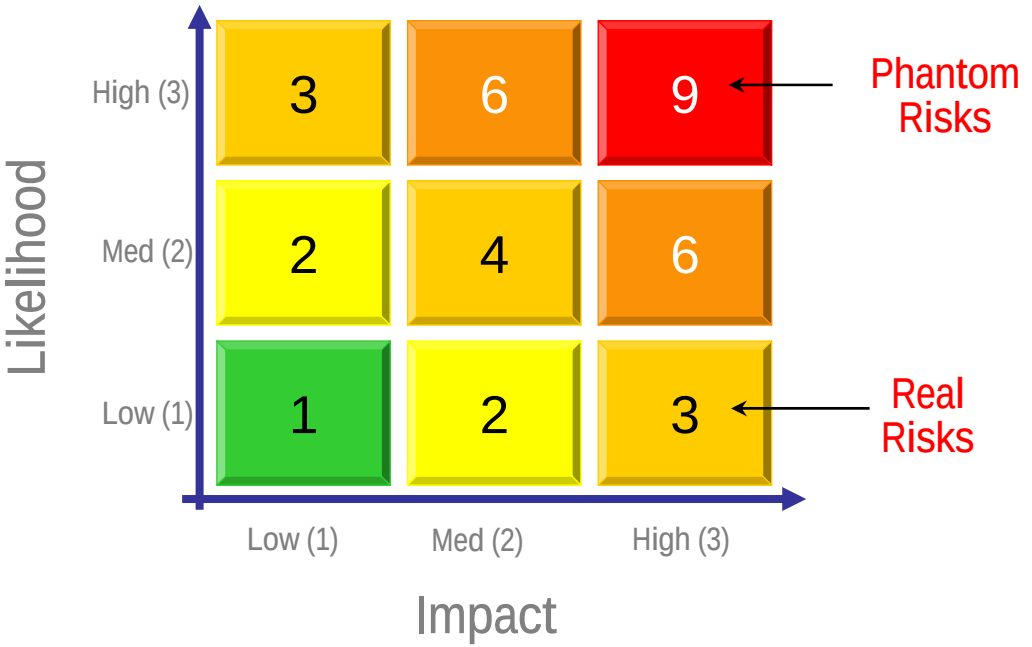


When compared, there are significant differences ….

MODERN



TRADITIONAL



Using likelihood-impact analysis one can calculate multiple outcomes.

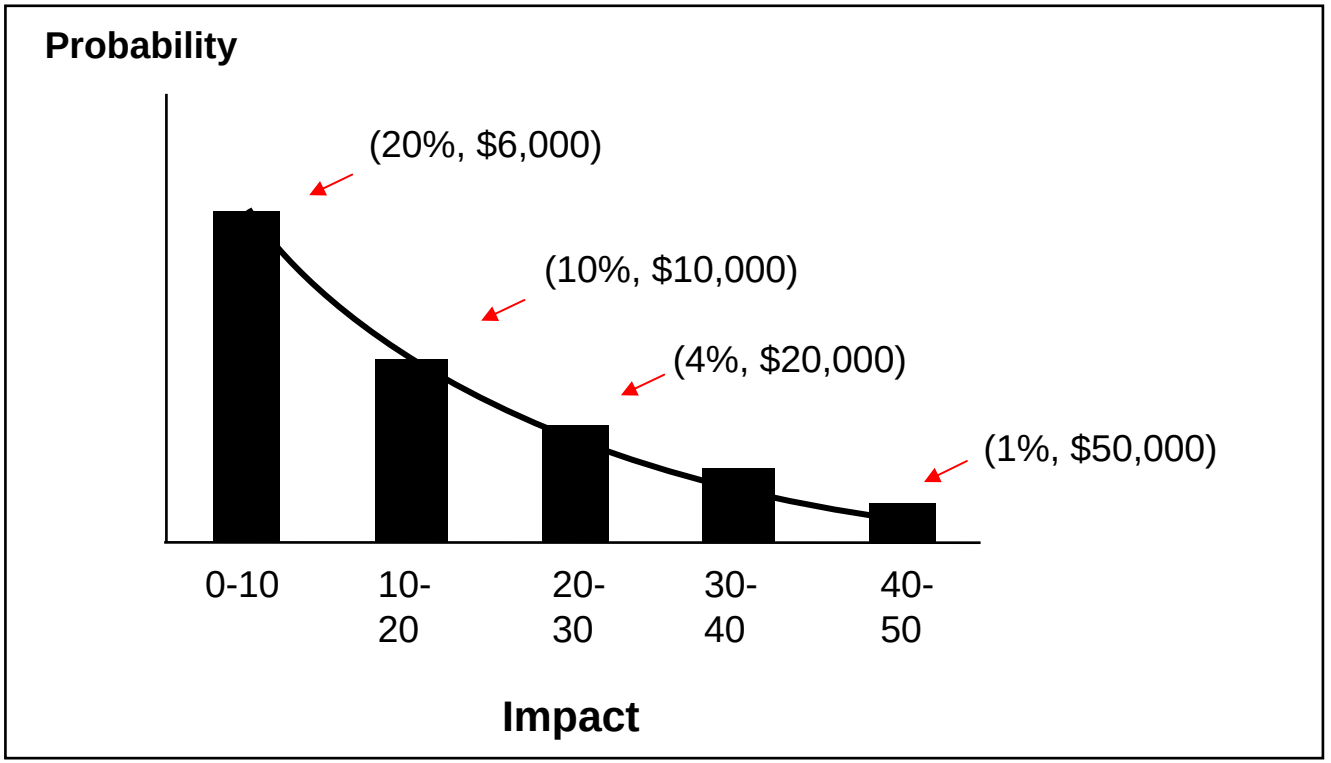
Likelihood x Impact = Risk

Risk 1 : 10% x $10,000 = $1,000
Risk 2 : 1% x $50,000 = $ 500

.
.
.
.

Risk 999 : 4% x $20,000 = $ 800
Risk 1000 : 20% x $ 6,000 = $1,200

The many probability and impact combinations represent a continuum.

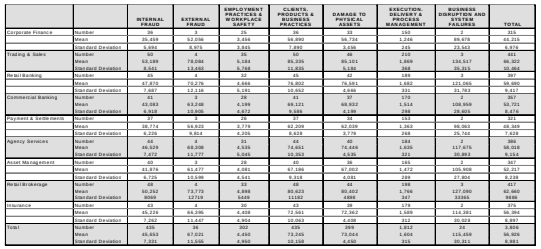


The severity distribution is a plot of all likelihood and impact combinations; loss severity is only one component of aggregate loss.

INDIVIDUAL LOSS EVENTS

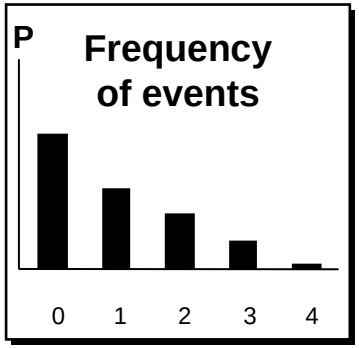
74,712,345
74,603,709
74,457,745
74,345,957
74,344,576
•
•
•
167,245
142,456
123,345
113,342
94,458

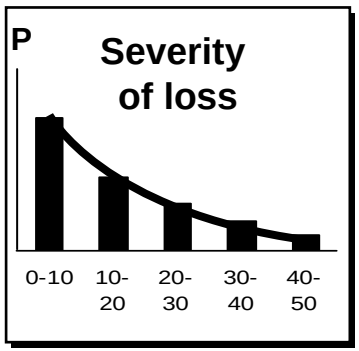
RISK MATRIX FOR LOSS DATA



		INTERNAL FRAUD	EXTERNAL FRAUD	EMPLOYMENT PRACTICES & WORKPLACE SAFETY	CLIENTS, PRODUCTS & BUSINESS PRACTICES	DAMAGE TO PHYSICAL ASSETS	EXECUTION, DELIVERY & PROCESS MANAGEMENT	BUSINESS DISRUPTION AND SYSTEM FAILURES	TOTAL
Corporate Finance	Number	26	1	25	25	18	130	1	315
	Mean	35,499	57,096	3,466	54,890	56,734	1,246	66,978	64,315
	Standard Deviation	5,484	8,971	3,845	7,890	3,438	241	23,523	6,878
Trading & Sales	Number	50	4	26	50	46	210	3	441
	Mean	53,189	78,086	6,194	85,206	86,101	1,869	134,517	96,322
	Standard Deviation	8,543	13,460	5,768	11,835	5,136	368	35,315	10,364
Retail Banking	Number	45	4	32	45	42	189	3	397
	Mean	47,870	73,276	4,666	74,802	76,591	1,682	121,065	86,660
	Standard Deviation	7,687	12,116	5,191	10,652	4,646	331	31,783	9,417
Commercial Banking	Number	41	3	26	41	37	170	2	367
	Mean	43,083	63,248	4,199	68,121	68,932	1,514	109,969	78,701
	Standard Deviation	6,919	10,906	4,672	9,586	4,139	299	28,561	8,470
Payment & Settlements	Number	37	3	29	37	34	153	2	321
	Mean	38,774	59,923	3,779	63,209	62,026	1,363	99,063	68,369
	Standard Deviation	6,226	9,614	4,255	8,829	3,729	268	25,744	7,828
Agency Services	Number	44	4	31	44	40	184	3	366
	Mean	46,529	68,208	4,535	74,661	74,449	1,635	117,675	84,018
	Standard Deviation	7,472	11,777	5,540	10,302	4,535	321	30,893	9,114
Asset Management	Number	40	3	28	40	36	165	2	347
	Mean	41,874	61,477	4,081	67,186	67,002	1,472	105,908	82,217
	Standard Deviation	6,725	10,595	4,541	9,318	4,041	289	27,801	8,218
Retail Brokerage	Number	49	4	33	48	44	198	3	417
	Mean	50,252	73,773	4,898	80,623	80,402	1,766	127,690	92,960
	Standard Deviation	8069	12719	5449	11182	4896	347	33361	9896
Insurance	Number	43	4	30	43	39	179	2	370
	Mean	45,226	66,396	4,408	72,561	72,362	1,589	114,381	96,384
	Standard Deviation	7,262	11,447	4,964	10,063	4,408	312	30,824	8,947
Total	Number	435	34	302	435	399	1,812	24	3,899
	Mean	45,453	67,071	4,450	73,245	73,043	1,601	116,456	86,906
	Standard Deviation	7,331	11,546	4,966	10,158	4,450	315	30,311	8,961

LOSS DISTRIBUTIONS

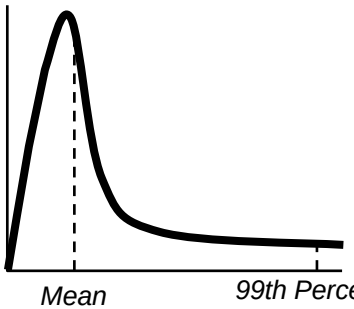




VAR CALCULATION

VaR Calculator e.g., Monte Carlo Simulation Engine

TOTAL LOSS DISTRIBUTION



Annual Aggregate Loss ($)

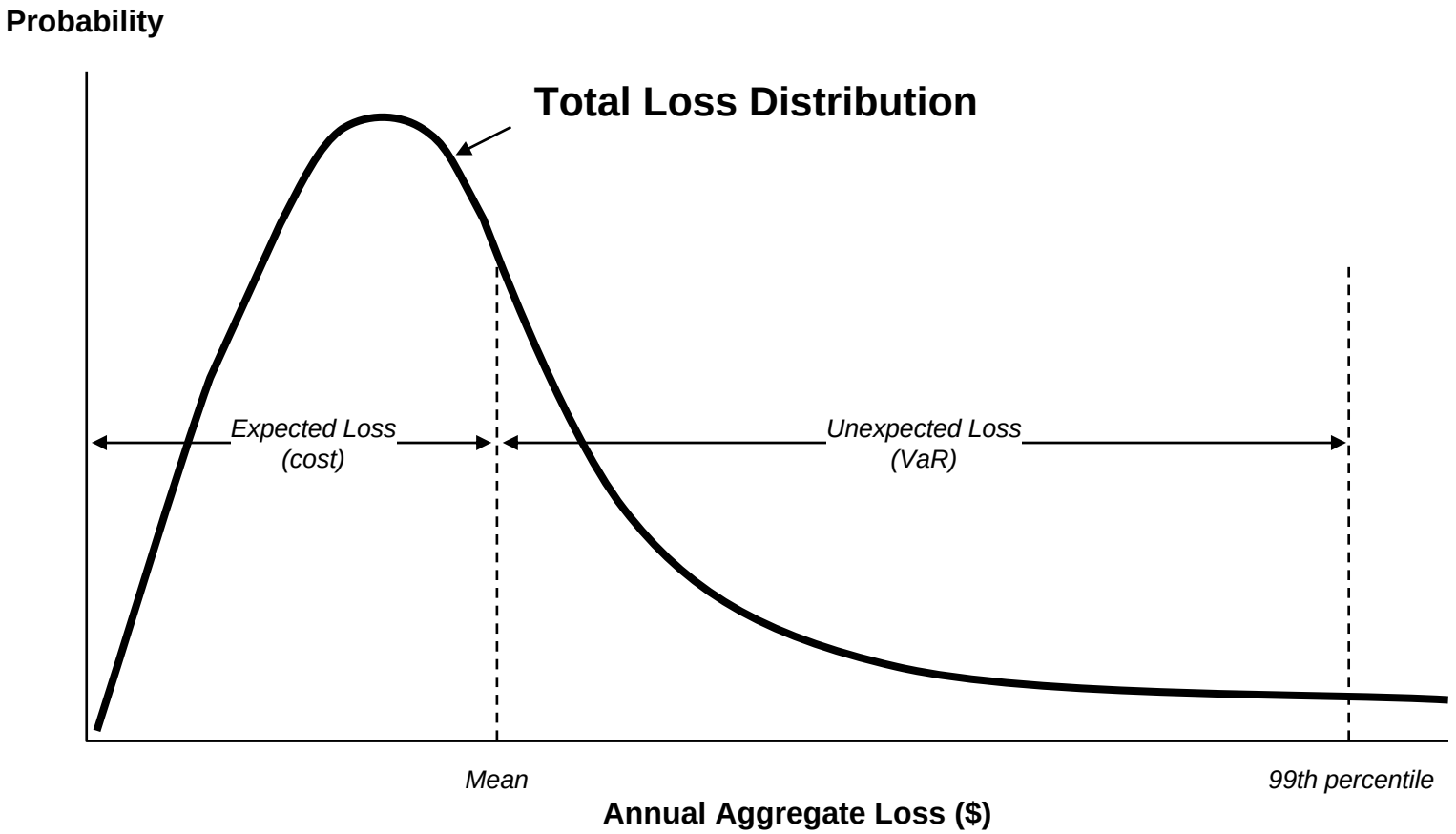
A high likelihood – high impact scenario: You are standing on the train tracks. 90% chance you will be hit by a train; impact $1,000,000.

- There can be a high likelihood-high impact scenario situations, but not a high likelihood-high severity class of events.
- Likelihood-impact analysis allows you to measure the probability weighted impact of a specific event – in other words the cost or damage from the event ($900,000).
- The risk represents the uncertainty surrounding the $900,000 damage estimate.
- As likelihood approaches 1.0 (100%), the event becomes certain and the risk goes to zero.

Additional comments about likelihood-impact analysis.

- Likelihood means probability; frequency means number of events.
- Likelihood and impact analysis is used for a specific, single incident (a point in time assessment).
- Frequency and severity distributions are used to describe characteristics of a risk class, where multiple incidents can take place during a given time period.
- Likelihood-impact analysis is more appropriate for operations management not operational risk management. In a crisis one is trying to measure the magnitude of one potential routine loss that is on the verge of taking place.

A cultural shift is necessary for practitioners to understand that risk is impact at a specified likelihood (e.g., 1% likelihood or 99% confidence level), not the product of likelihood and impact or frequency and impact.



Suppose a bank is not planning on adopting the AMA, is it necessary for that bank to adopt a probabilistic concept of risk?

C. Qualifying criteria

1. The Standardised Approach[100]

660. In order to qualify for use of the Standardised Approach, a bank must satisfy its supervisor that, at a minimum:

- Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;
- It has an operational risk management system that is conceptually sound and is implemented with integrity; and

There is only one definition of risk.

Not separate (custom) definitions for the BIA, the TSA and the AMA.

Is it practical to require all banks to follow this definition of risk?

Issue: How can a probabilistic concept of risk be applicable to ORM, where very little data is available and quantitative modeling (which relies on large amounts of data) is impractical? Instead, why not use expert judgment which can be used in situations were there is very little data?

Answer: A probabilistic approach does not necessarily imply large databases or sophisticated tools. Even in cases where very little information is available, and where expert assessments are the only practicable solution, a probabilistic approach can be used to ask better, more unambiguous questions.

For example, in conventional approaches, experts are typically asked “what is the likelihood and impact of event x occurring over a one year horizon?” Unfortunately, some experts will mentally reflect “in a normal/average situation”, some optimists in a “not so bad” situation and other may consider a “disaster” scenario. As a result, nobody can accurately interpret the answers of make meaningful use of the results. A probabilistic approach could simply mean asking a smarter set of questions.

Source/inspiration: Jean-Charles Sevet, ECB

How does a risk manager conceptualize an ORM problem?

- A Bank has a computer system that goes down frequently - on average about five hours per week. No one can work productively while the system is down. Should the bank purchase a new system which costs $5,000,000?

  •Accountant: Estimate the total cost of employee time lost (five hours per employee, per week).

  •Economist: Estimate the amount of profit that could be generated (opportunity cost) if the employees were able to work more productively.

  •Risk Manager: Five hours is the average; what happens in the “worst case” situation? What mission critical tasks will fail to be performed when this happens and what will that cost (in direct losses and opportunity cost).

An example of an effective use of ORM in the business decision making process.

- Consider two risks: Unauthorized Trading and Money Transfer
- Past Audits reveal that both risks are under-controlled
- To address Unauthorized Trading risk one must improve segregation of duties and audit frequency. (Solution: hire four new staff; cost = $400,000 per year)
- To address Money Transfer risk one must improve the system (Solutions: buy new system; cost = $5 million + $800,000 per year)
- You have $4 million in your budget. Where do you invest your money?

At the 99.X% level, how much risk do you have in money transfer vs. unauthorized trading?

Suppose you had tried to solved this problem by using internal loss data, or by generating scenario loss data or by tracking KRIs?

Why do we care so much about the large, infrequent losses?

- The large events have a huge impact, not just on solvency, but also on annual financial performance.
  - One percent of the events cause 60-70% of the losses.
    - Therefore a large part of the average cost of operational failure (the expected loss) comes from the extreme events.
  - How many people die on average each year as a result of drowning? (now factor in tsunami drownings).
- Successfully managing operational risk is critically dependent on preventing major losses from taking place and/or reducing potential damage from such events.

An example of an effective use of ORM in the business decision making process.

A seafood processor want to build a new $30M plant. There are two options:

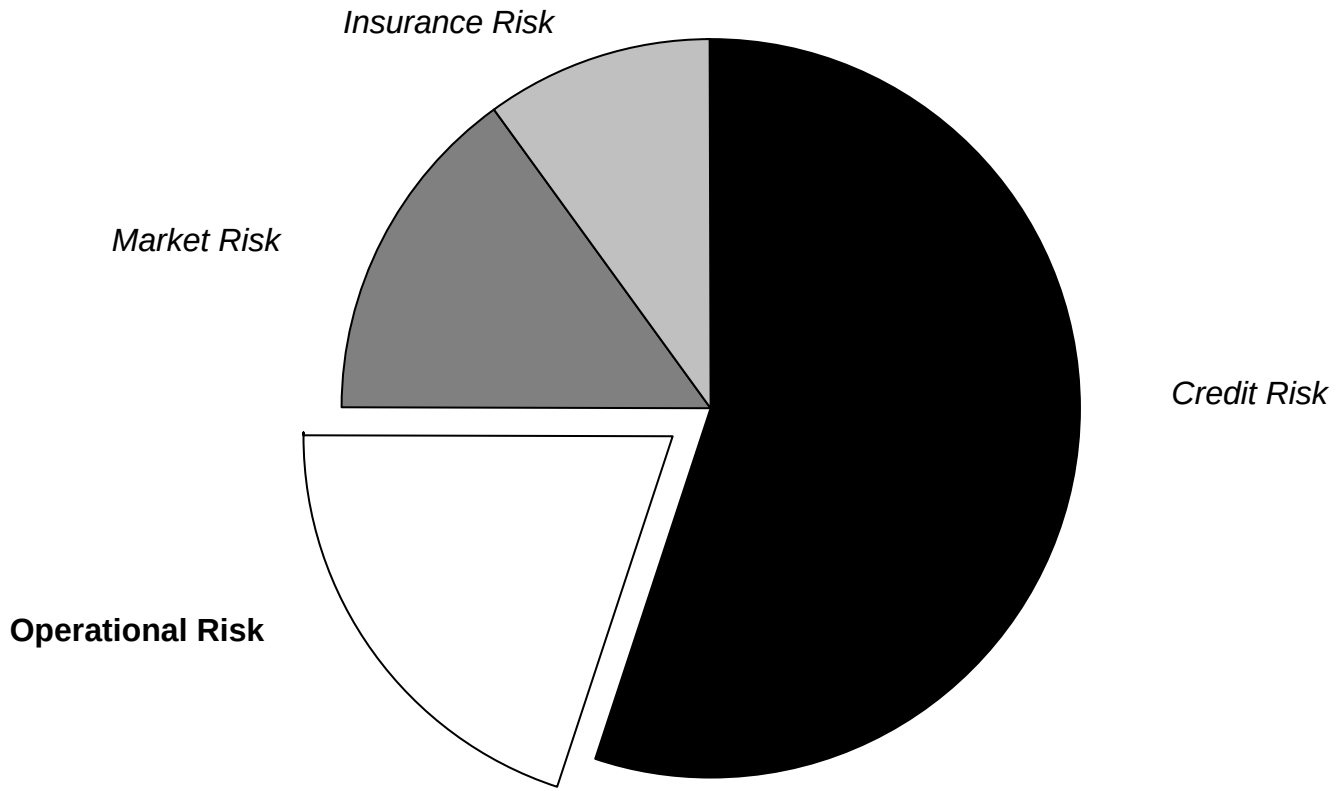
Build the plant on the banks of a river that floods roughly once in every 20 years. Estimated annual profit is $5M.

Build the plant on a nearby hill and incur additional annual operating costs of $1M per year. Estimated annual profit is $4M.

Are the goals of business line management
the same as those of the board of directors?

WHAT ARE RISKS & CONTROLS?

Many years ago we defined operational risk as all risk other than market, credit and insurance risk.



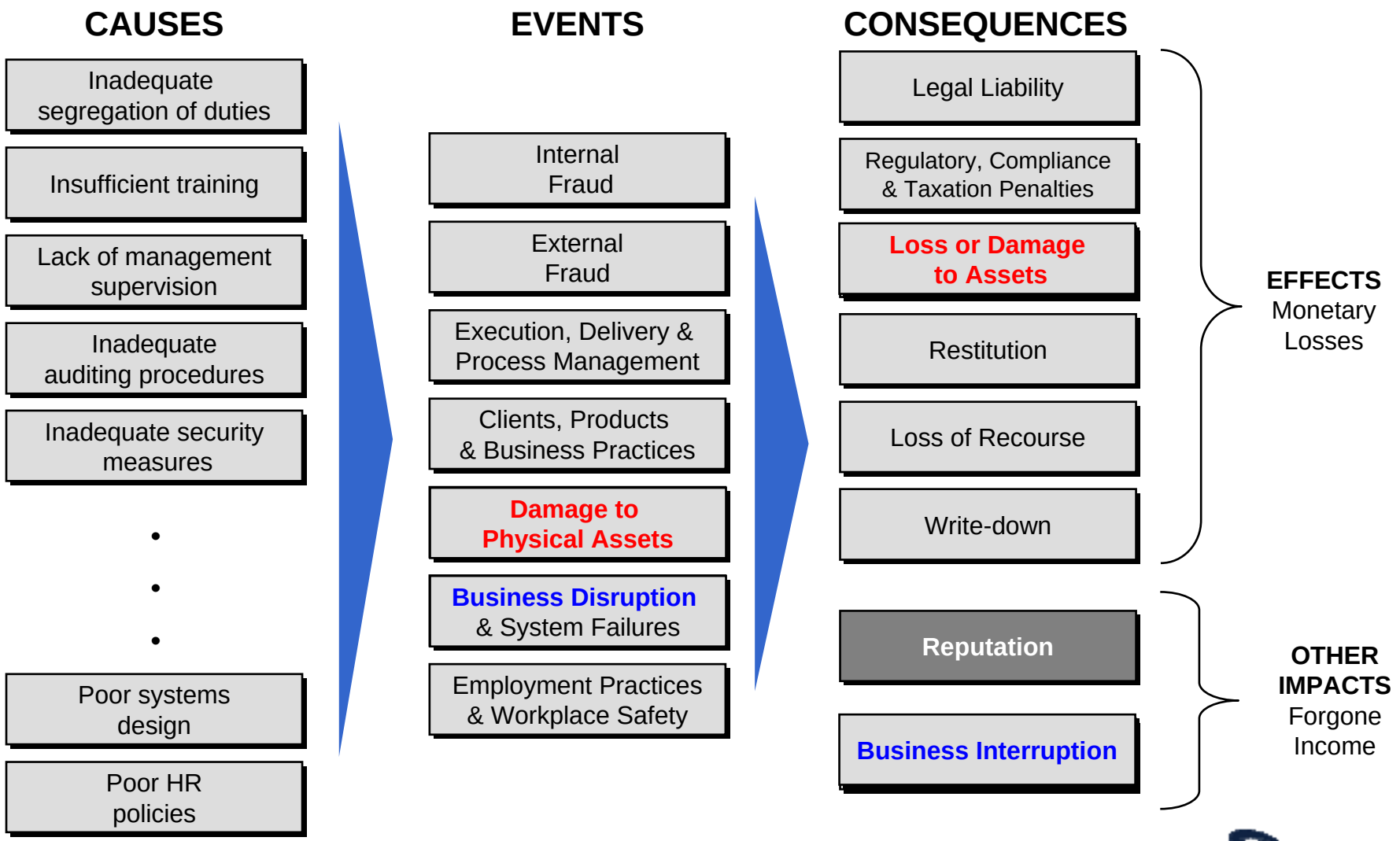
What comprises operational risk?

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

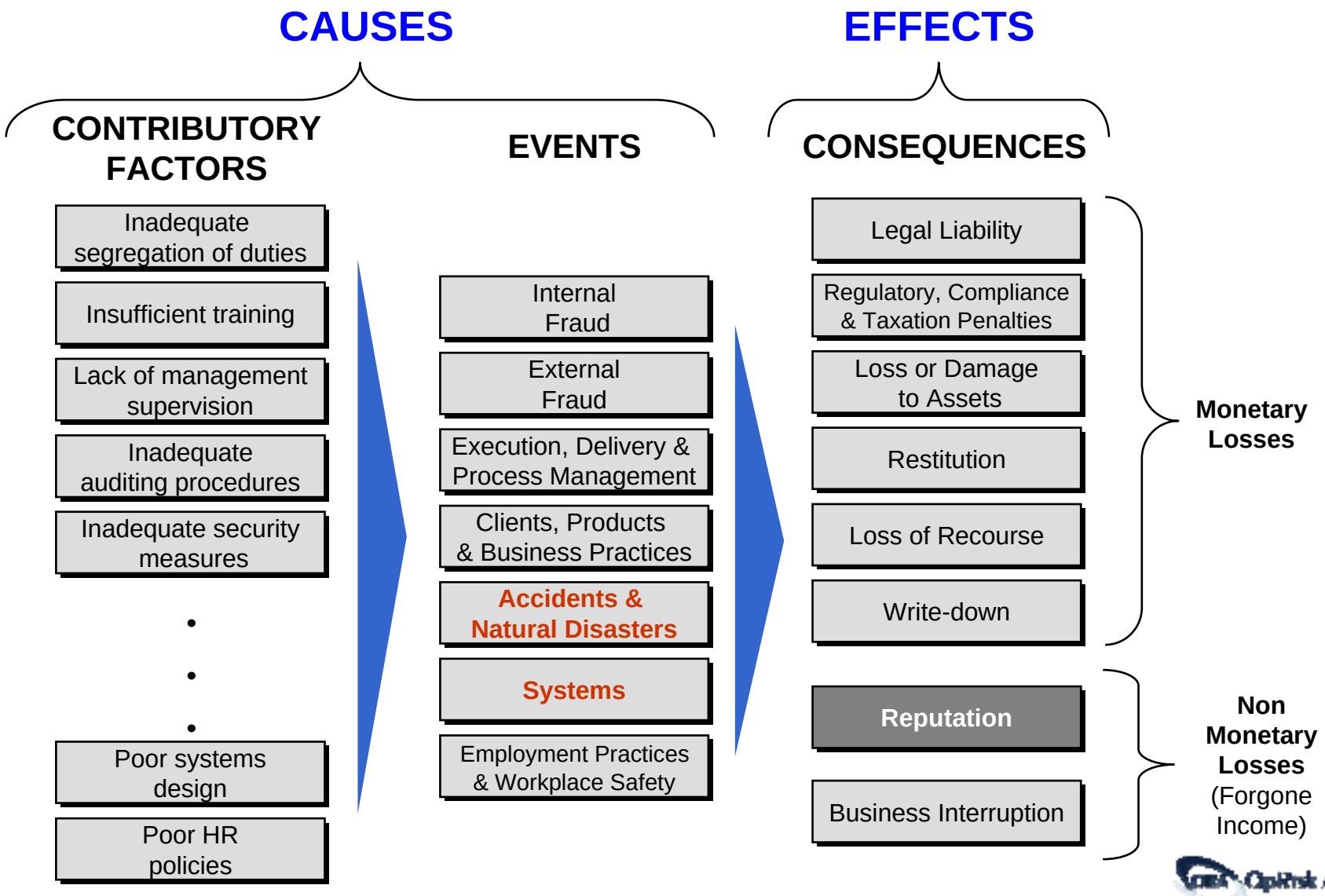
Effective ORM requires a structured way of thinking about risk – a meaningful way of conceptualizing the issues and a common language. What are the standards for defining and categorizing operational risk?

Management Information	Grouping of like items (homogenous risk types) to facilitate the management of similar issues which have similar inherent characteristics (risk profiles) and causes (controls).
Statistical Consistency	Mutually exclusive (no overlaps) and exhaustive (comprehensive) homogenous distributions
Logical Consistency	Must be based on natural boundaries; examples must be consistent with definitions

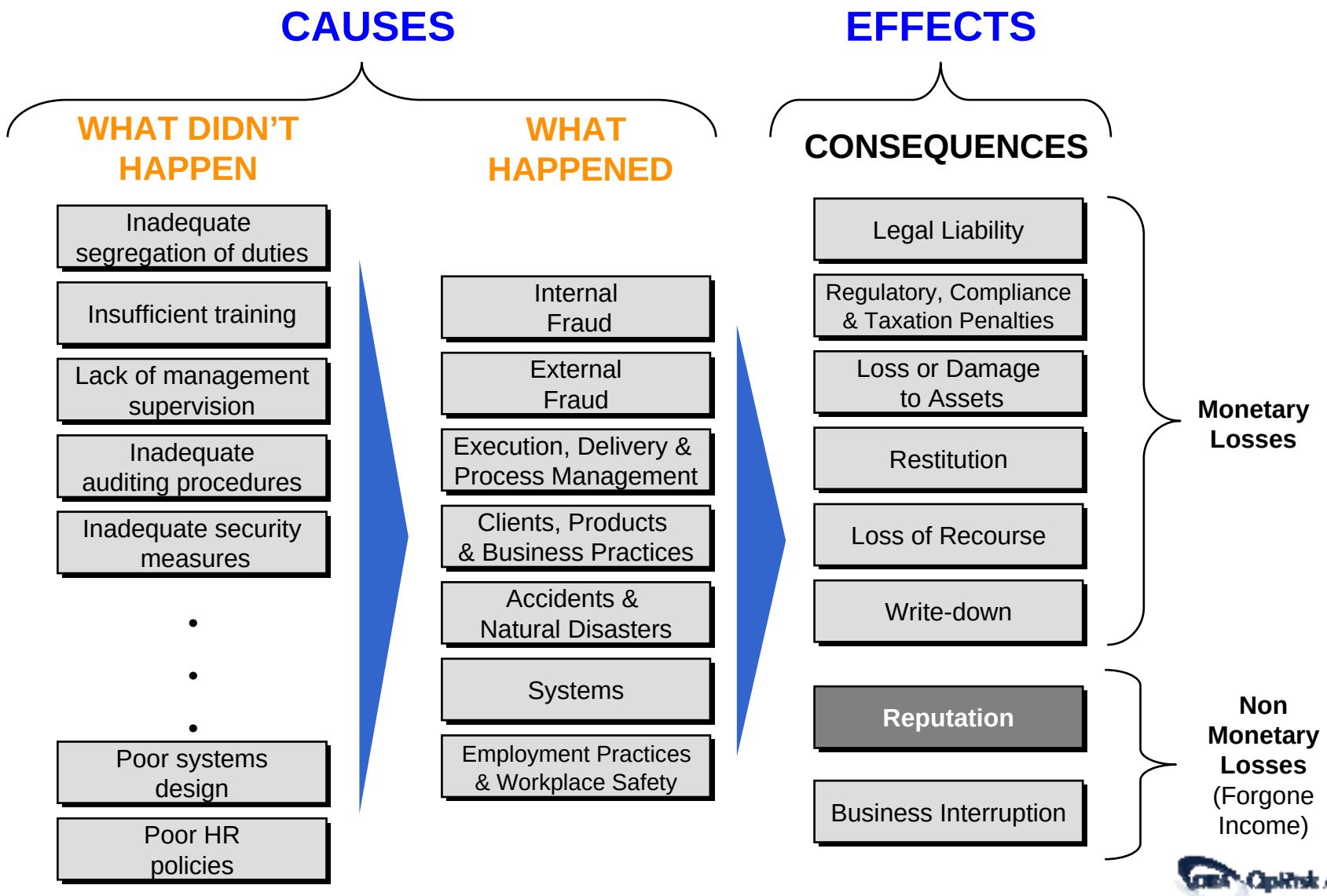
The universe of operational risk is best understood in terms of its three dimensions: causes, events and consequences. The Basel II event based framework appears to have some inconsistencies.



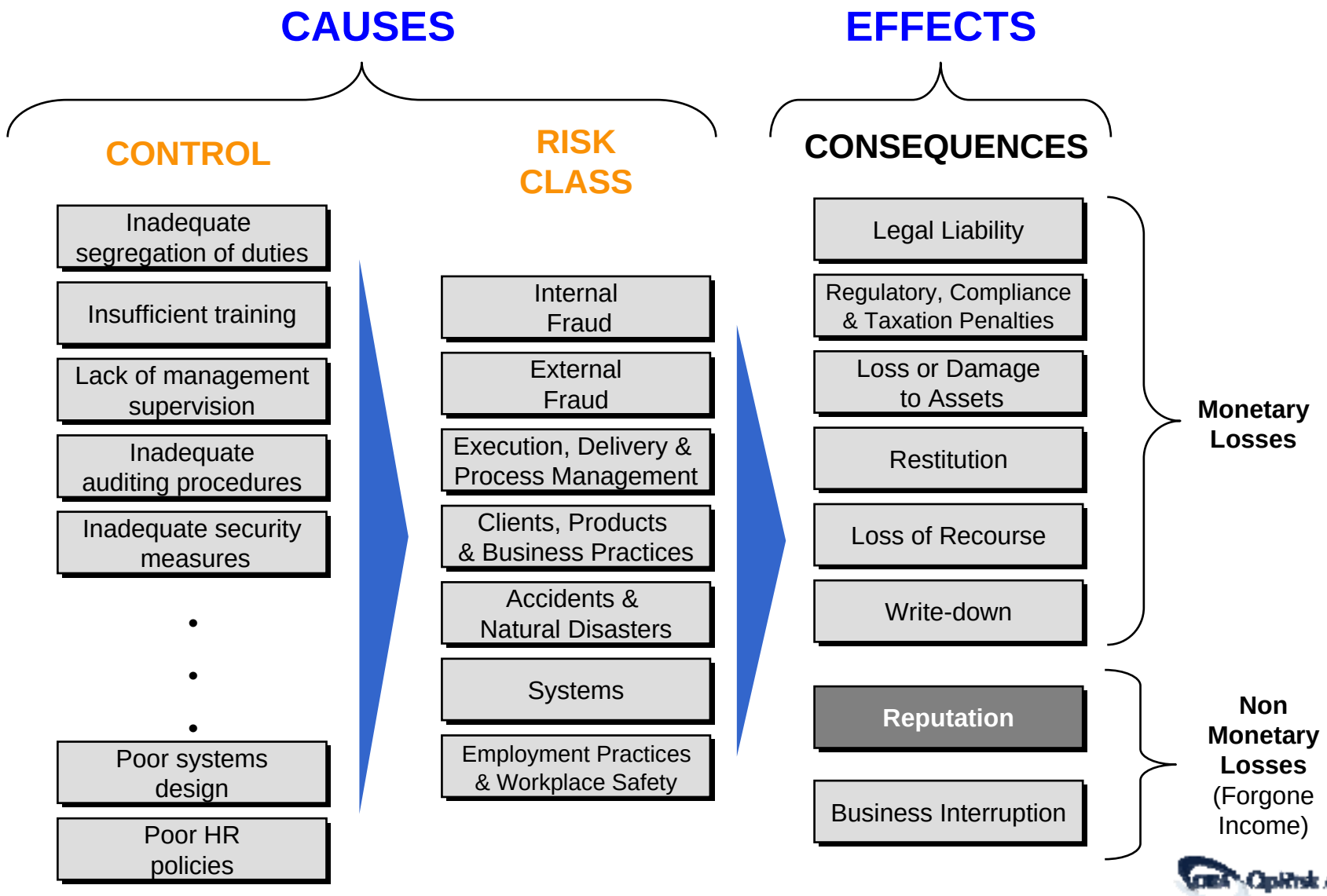
Upon further analysis, it appears that “causes” consist of both contributory factors and events (contributory factors and events together cause losses).



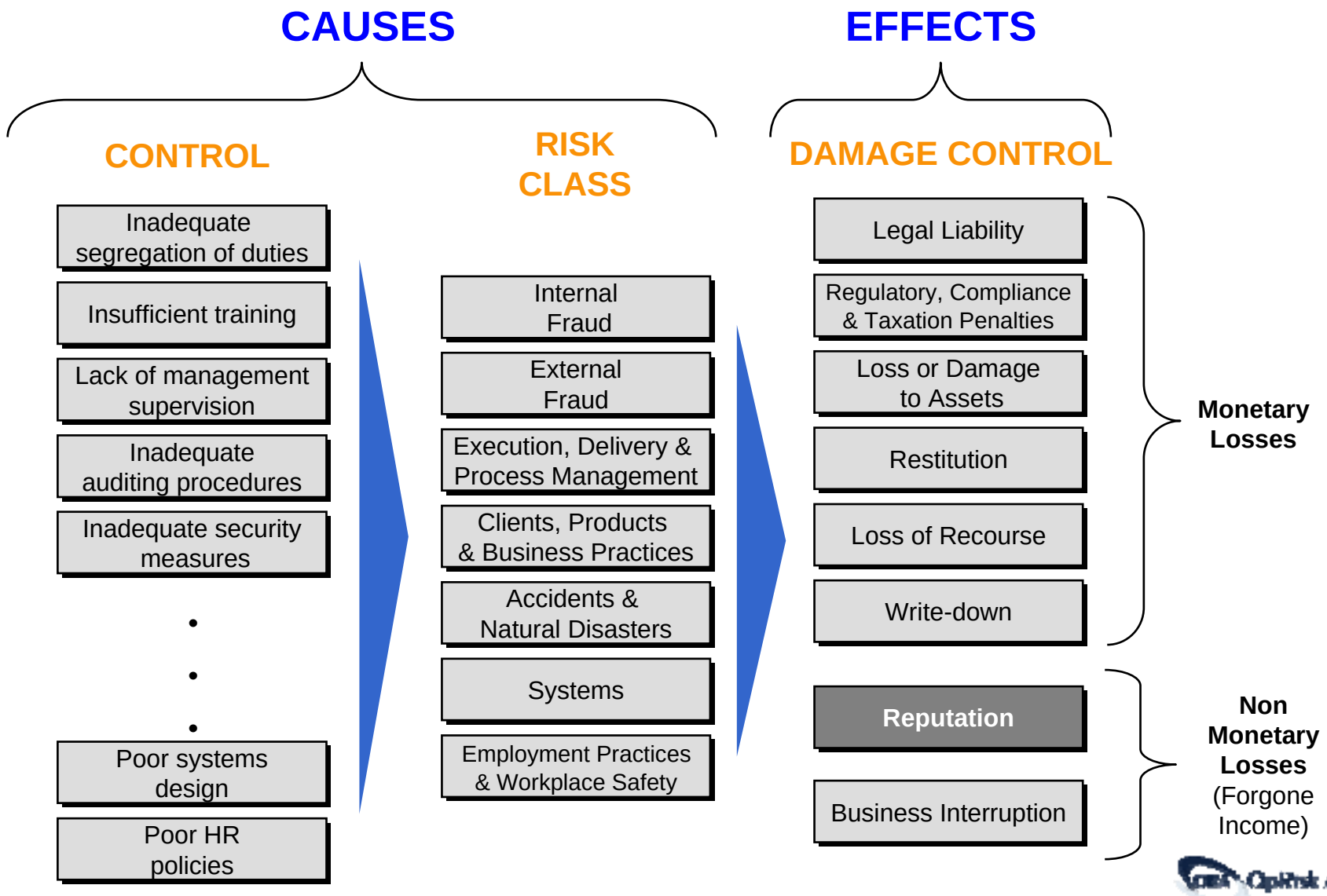
Contributory factors are things that should have been done, but weren't done (nothing has necessarily happened). Events represent something that happened (e.g., a loss).



Contributory factors are really controls. Events represent classes of "inherent" risk types. Events are not directly controllable.



Contributory factors are really controls. Events represent classes of "inherent" risk types. Events are not directly controllable.



Event risk categories are represented in a three-tier hierarchy.

Primary	Secondary	Activity Examples
Internal Fraud *Losses due to acts of type intended to defraud misappropriate property, or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party*	Unauthorized Activities	Transactions not reported (intentional), Transaction type unauthorized (w/monetary loss), Mismarking of position (intentional)
	Theft & Fraud	Fraud/credit fraud, worthless deposits, Theft, extortion, embezzlement, robbery, Misappropriation of assets, Malicious destruction of assets, Forgery, Check kiting, Smuggling, Accountant takeover, impersonation, Tax noncompliance, evasion (willful), Bribes/Kickbacks, Insider trading (not on firm's account)
External Fraud *Losses due to acts of type intended to defraud, misappropriate property, or circumvent regulations, or the law by a third party*	Theft & Fraud	Theft/Robbery Forgery Check kiting
	Systems Security	Hacking damage, Theft of information (w/monetary loss)
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.*	Employee Relations	Compensation, benefit, termination issues, Organized labor activity, Poaching
	Safe Environment	General liability (slip and fall, etc), Employee health & safety rules events, Workers' compensation
	Diversity and Discrimination	All forms of discrimination

Event risk categories are represented in a three-tier hierarchy (continued).

Primary	Secondary	Activity Examples
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.*	Suitability, Disclosure & Fiduciary	Fiduciary breaches - guideline violations, Suitability - disclosure issues (know your customer etc.), Retail consumer disclosure violations, Breach of privacy, Aggressive sales, Account churning, Misuse of confidential information, Lender liability,
	Selection, Sponsorship & Exposure	Failure to investigate client per guidelines, Exceeding client exposure limits
	Advisory Activities	Disputes over performance of advisory activities
	Improper Business or Market Practices	Antitrust, Improper trade/market practices, Market manipulation, Insider trading (on firm's account), Unlicensed activity, Money Laundering
	Product Flaws	Product defects (unauthorized), Model errors
Damage to Physical Assets *Losses arising from loss or damage to physical assets from natural disaster or other events.*	Disasters and other events	Natural disaster losses, Human losses from external sources (terrorism, vandalism)
Business Disruption and System Failures *Losses arising from disruption of business or systems failures*	Systems	Hardware, Software, Telecommunications, Utility outage/disruptions

Event risk categories are represented in a three-tier hierarchy (continued).

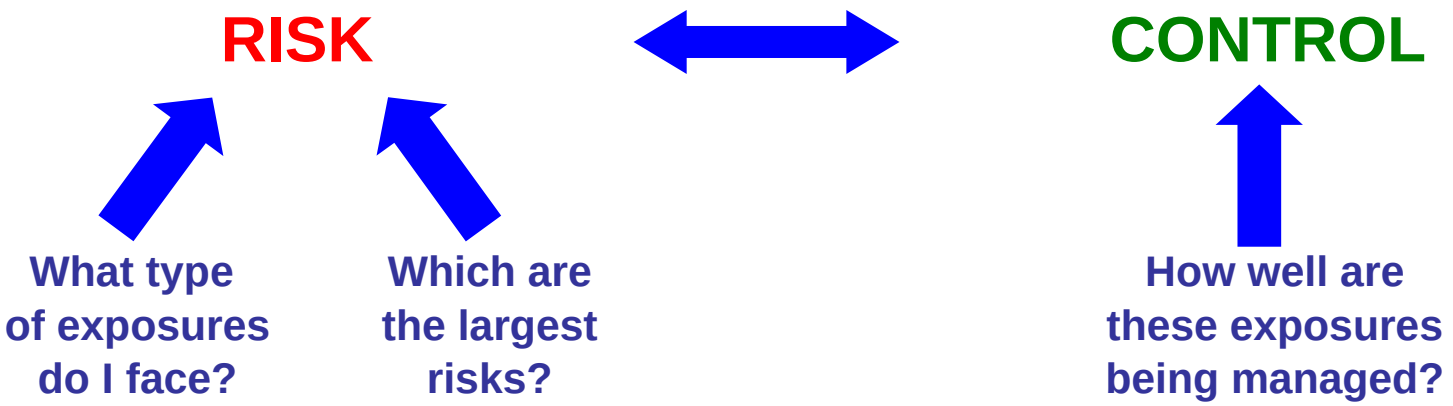
Primary	Secondary	Activity Examples
Execution, Delivery & Process Management *Losses from failed transaction processing or process management, from relations with trade counter parties and vendors or from systems failures.*	Transaction Capture, Execution & Maintenance	Miscommunication, Data entry, maintenance, or loading error, Missed deadline or responsibility, Model/system misoperation, Accounting error, entity attribution error, Other task misperformance, Delivery failure, Collateral management failure, Reference data maintenance
	Monitoring and Reporting	Failed mandatory reporting obligation, Inadequate oversight, Inaccurate external report (loss incurred)
	Customer Intake and Documentation	Client permissions, disclaimers missing, Legal documents missing, incomplete
	Customer/Client Account Management	Unapproved access given to accounts (includes inadvertent access to one party on a joint account) Incorrect client records (loss incurred), Negligent loss or damage of client assets
	Trade Counter parties	Nonclient counter party misperformance, Misc. nonclient counter party disputes
	Vendors and Suppliers	Outsourcing, Vendor disputes

The starting point for diagnostic analysis is the Business Line/Event Risk matrix. Using loss data in the context of this matrix one can discover where one's risks really exist (risk identification).

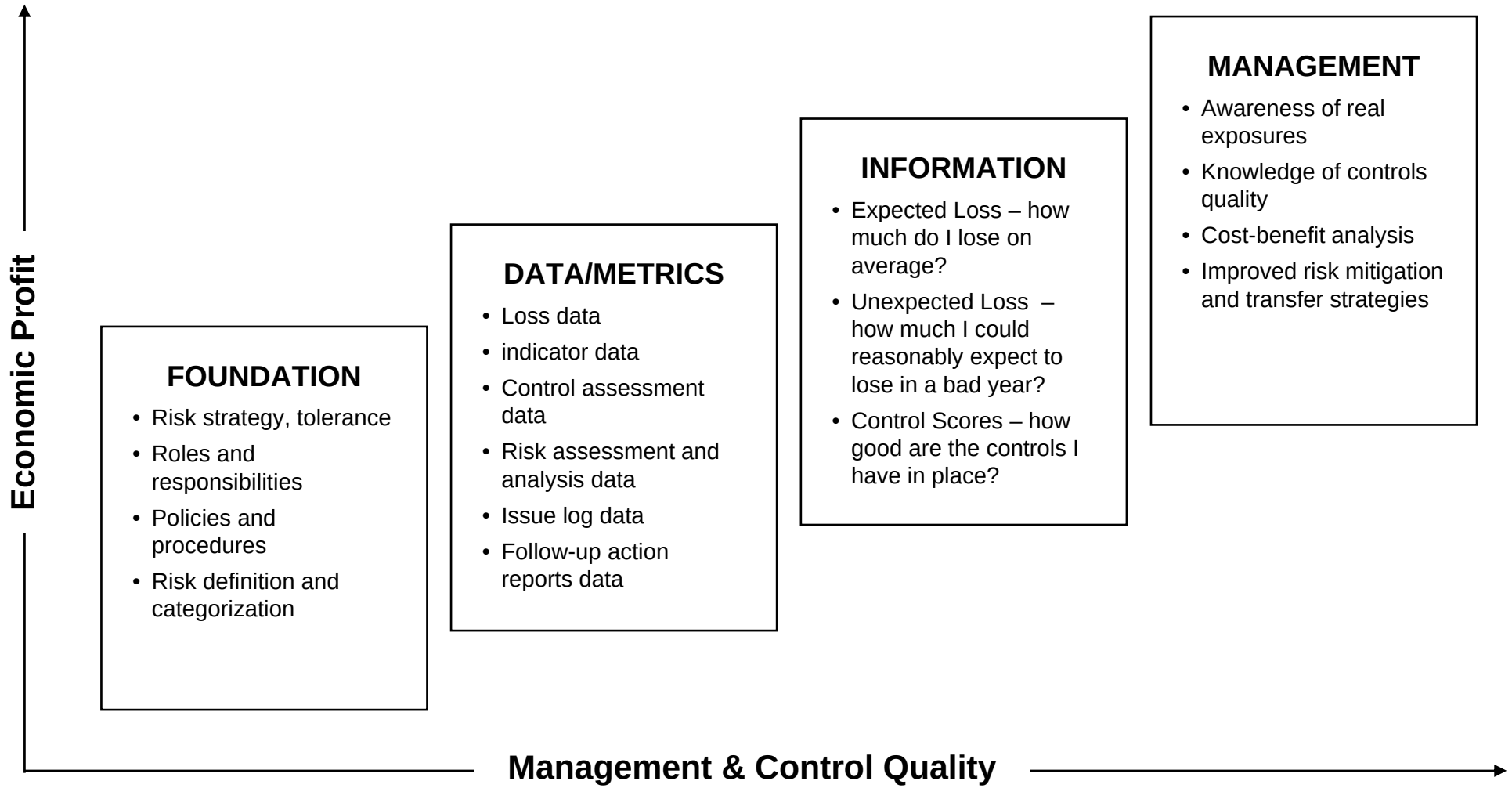
		INTERNAL FRAUD	EXTERNAL FRAUD	EMPLOYMENT PRACTICES & WORKPLACE SAFETY	CLIENTS, PRODUCTS & BUSINESS PRACTICES	DAMAGE TO PHYSICAL ASSETS	EXECUTION, DELIVERY & PROCESS MANAGEMENT	BUSINESS DISRUPTION AND SYSTEM FAILURES	TOTAL
Corporate Finance	Number	362	123	25	36	33	150	2	731
	Mean	35,459	52,056	3,456	56,890	56,734	1,246	89,678	44,215
	Standard Deviation	5,694	8,975	3,845	7,890	3,456	245	23,543	6,976
Trading & Sales	Number	50	4	35	50	46	210	3	398
	Mean	53,189	78,084	5,184	85,335	85,101	1,869	134,517	66,322
	Standard Deviation	8,541	13,463	5,768	11,835	5,184	368	35,315	10,464
Retail Banking	Number	45	4	32	45	42	189	3	360
	Mean	47,870	70,276	4,666	7,802	76,591	1,682	121,065	59,690
	Standard Deviation	7,687	12,116	5,191	10,[illegible]2	4,666	331	31,783	9,417
Commercial Banking	Number	41	3	28	[illegible]1	37	170	2	322
	Mean	43,083	63,248	4,199	9,[illegible]1	68,932	1,514	108,959	53,721
	Standard Deviation	6,918	10,905	4,672	[illegible]86	4,199	298	28,605	8,476
Payment & Settlements	Number	37	3	26	37	34	153	2	292
	Mean	38,774	56,923	3,[illegible]79	62,209	62,039	1,363	98,063	48,349
	Standard Deviation	6,226	9,814	2[illegible]	8,628	3,779	268	25,744	7,628
Agency Services	Number	44	4	[illegible]	44	40	184	2	349
	Mean	46,529	68,308	4,535	74,651	74,446	1,635	117,675	58,018
	Standard Deviation	7,472	11,777	5,045	10,353	4,535	321	30,893	9,154
Asset Management	Number	40	3	28	40	36	165	2	314
	Mean	41,876	61,477	4,081	67,186	67,002	1,472	105,908	52,217
	Standard Deviation	6,725	10,599	4,541	9,318	4,081	289	27,804	8,238
Retail Brokerage	Number	48	4	33	48	44	198	3	378
	Mean	50,252	73,773	4,898	80,623	80,402	1,766	127,090	62,660
	Standard Deviation	8069	12719	5449	11182	4898	347	33365	9886
Insurance	Number	43	4	30	43	39	179	2	340
	Mean	45,226	66,395	4,408	72,561	72,362	1,589	114,381	56,394
	Standard Deviation	7,262	11,447	4,904	10,063	4,408	312	30,028	8,897
Total	Number	710	152	268	384	351	1,598	21	3,484
	Mean	45,653	67,021	4,450	73,245	73,044	1,604	115,459	56,926
	Standard Deviation	7,331	11,555	4,950	10,158	4,450	315	30,311	8,981

WHAT IS MODERN ORM?

REVIEW: Operational risk management is the process of optimizing the risk-control relationship in the context of cost-benefit analysis.



Effectively managing operational risk requires a framework designed to turn raw operational risk data into information that supports managerial decision making.

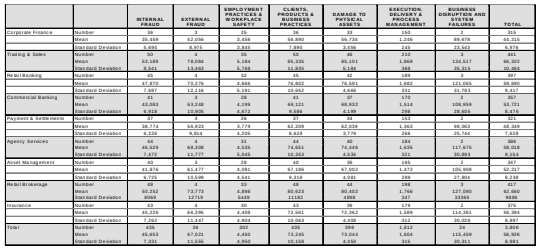


Since operational risk is measured in terms of the aggregate loss, there are two components to operational risk: Frequency and Severity. Unlike in market and credit risk there is no upper limit in operational risk.

INDIVIDUAL LOSS EVENTS

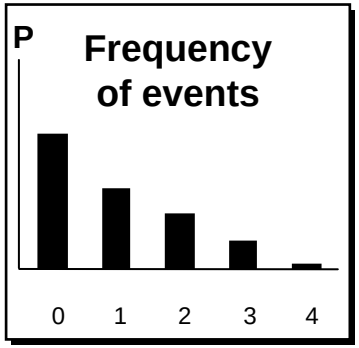
74,712,345
74,603,709
74,457,745
74,345,957
74,344,576
•
•
•
167,245
142,456
123,345
113,342
94,458

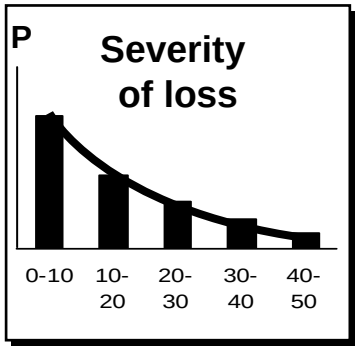
RISK MATRIX FOR LOSS DATA



		INTERNAL FRAUD	EXTERNAL FRAUD	EMPLOYMENT PRACTICES & WORKPLACE SAFETY	CLIENTS, PRODUCTS & BUSINESS PRACTICES	DAMAGE TO PHYSICAL ASSETS	EXECUTION, DELIVERY & PROCESS MANAGEMENT	BUSINESS DISRUPTION AND SYSTEM FAILURES	TOTAL
Corporate Finance	Number	20	1	21	61	18	190	4	315
	Mean	35,499	57,096	3,446	94,890	94,734	1,246	86,978	64,315
	Standard Deviation	5,484	8,971	3,845	7,892	3,436	241	23,523	6,974
Trading & Sales	Number	50	4	26	50	46	210	3	443
	Mean	53,189	78,086	6,194	89,206	86,101	1,869	136,517	66,322
	Standard Deviation	8,563	13,460	5,768	11,835	5,136	368	35,315	10,364
Retail Banking	Number	45	4	32	65	62	169	2	397
	Mean	47,870	73,276	4,866	74,802	76,591	1,682	121,065	58,990
	Standard Deviation	7,687	12,116	5,191	10,952	4,846	331	31,783	9,417
Commercial Banking	Number	41	3	26	41	37	170	2	367
	Mean	43,083	63,248	4,199	68,121	68,922	1,514	108,969	53,701
	Standard Deviation	6,919	10,906	4,672	9,184	4,139	299	29,901	8,476
Payment & Settlements	Number	37	3	28	37	34	153	2	321
	Mean	38,774	59,923	3,779	63,209	62,026	1,363	99,063	48,369
	Standard Deviation	6,226	9,614	4,255	8,829	3,779	268	25,764	7,828
Agency Services	Number	44	4	21	44	40	184	3	396
	Mean	46,629	68,208	4,535	74,661	74,449	1,635	117,675	58,018
	Standard Deviation	7,472	11,777	5,245	10,353	4,535	321	30,893	9,114
Asset Management	Number	40	3	29	40	36	165	2	347
	Mean	41,874	61,477	4,081	67,186	67,002	1,472	105,908	52,217
	Standard Deviation	6,725	10,595	4,541	9,318	4,081	289	27,864	8,204
Retail Brokerage	Number	48	4	33	48	44	198	3	417
	Mean	50,252	73,773	4,898	80,823	80,402	1,766	127,690	62,960
	Standard Deviation	8069	12719	5449	11182	4896	347	33361	9896
Insurance	Number	43	4	30	43	39	179	2	370
	Mean	45,226	66,396	4,408	72,581	72,362	1,589	114,381	56,364
	Standard Deviation	7,262	11,447	4,904	10,063	4,408	312	30,819	8,947
Total	Number	435	34	302	435	399	1,812	24	3,899
	Mean	45,453	67,071	4,450	73,245	73,043	1,601	110,459	56,926
	Standard Deviation	7,331	11,546	4,966	10,158	4,450	315	30,311	8,961

LOSS DISTRIBUTIONS

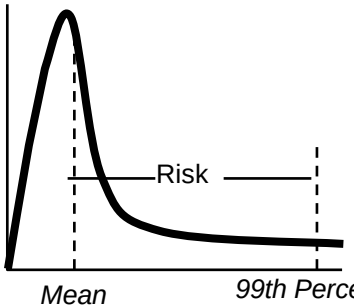




VAR CALCULATION

VaR Calculator e.g., Monte Carlo Simulation Engine

TOTAL LOSS DISTRIBUTION



Annual Aggregate Loss ($)

We then independently assess the quality of the internal controls, corresponding to each risk type, using the same business line/risk type matrix.

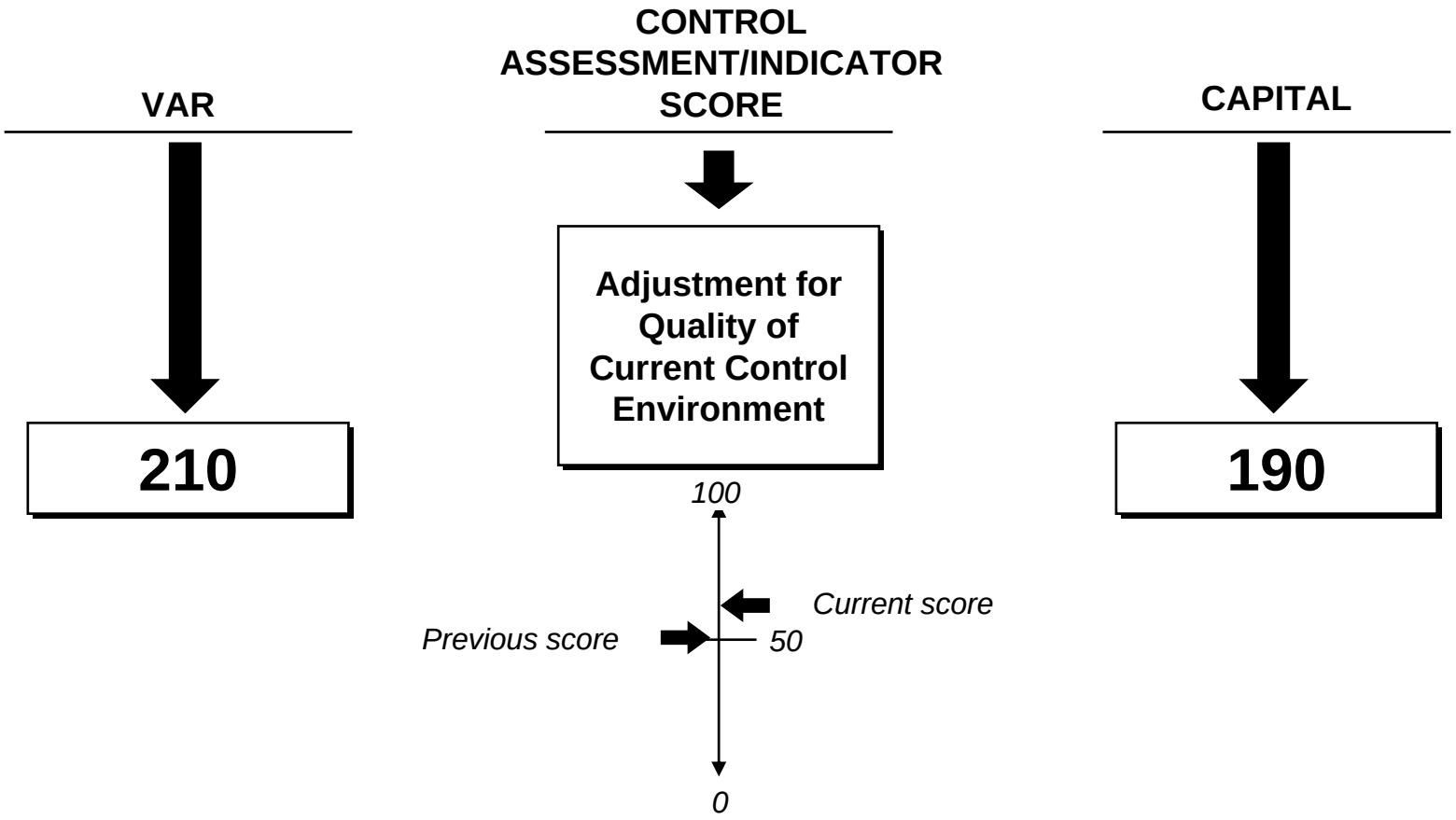
Aggregation Matrix	Business Disprution & System Failures	Clients, Products & Business Practices	Damage to Physical Assets	Employment Practices & Workplace Safety	Execution, Delivery & Process Management	External Fraud	Internal Fraud	Total Score
Chicago Equities	31	66	54	82	64	32	62	56
London Equities	76	46	90	50	52	84	39	62
Madrid Equities		96	34	86	89	56	70	68
New York Equities	74	30	56	33	49	54	96	56
Paris Equities	36	70	43	92	82	50	47	60
Singapore Equities	50	62	89	40	62	43	76	60
Bangkok Equities	45	32	76	32	74	86	56	57
Los Angeles Equities	52	57	63	59	67	58	63	60

Modern ORM follows an integrated approach, where risk and control information can be compared through a common view (e.g., a matrix).

INTEGRATED RISK & CONTROL MATRIX

		INTERNAL FRAUD	EXTERNAL FRAUD	EMPLOYMENT PRACTICES & WORKPLACE SAFETY	CLIENTS, PRODUCTS & BUSINESS PRACTICES	DAMAGE TO PHYSICAL ASSETS	EXECUTION, DELIVERY & PROCESS MANAGEMENT	BUSINESS DISRUPTION AND SYSTEM FAILURES	TOTAL
Corporate Finance	Previous VaR	21,000,000	36,000,000	62,000,000	75,000,000	124,000,000	86,000,000	36,000,000	362,000,000
	Prev/Current Score	50 55	60 58	75 71	61 61	45 55	50 52	50 55	50 55
	Final Capital	19,000,000	35,000,000	65,000,000	75,000,000	104,000,000	83,000,000	32,000,000	326,000,000

Risk metrics tend to be relatively static; control metrics could be used to predict changes in levels of risk. Used in conjunction with risk capital control metrics could be used to create the right incentives.



Linking capital to changes in the quality of internal controls provides an incentive for desired behavioral change

SUMMARY & CONCLUSIONS

What are the key challenges banks face in establishing a viable ORM framework?

- We have advised more than fifty banks, insurance companies, technology companies, multi-lateral organizations and national and international regulators in more than 25 countries in North America, Europe, Asia, Australia and Africa on the full range of operational risk measurement and management issues.
- Our observations:
  - Banks around the world are facing serious challenges in implementing ORM under Basel II.
  - Almost all banks are struggling with the same key issues.
  - Many have unknowingly adopted the wrong definition of risk.
  - Some use a probabilistic concept of risk in their models, but a different definition of risk in their broader framework, while ignoring the inherent contradiction.

Why are banks having such a difficult time implementing ORM?

- Many people who work in ORM don't understand elementary risk management concepts.
- Following the advice of numerous "experts" most banks have developed ORM frameworks based on a convoluted blend of traditional and modern ORM.
- Traditional ORM and Modern ORM are based on entirely different definitions, approaches, processes and methodologies.
- These immature methodologies are highly subjective, resource intensive and generate a huge catalog of unmanageable 'risks.'
- Any prioritization of controls based on this spurious and misleading information may lead managers to enhance controls in areas that are already over-controlled and at the same time ignore areas of major control weakness.

Key differences between Traditional and Modern ORM.

Traditional

Definition: Risk is defined as **a kind of unpleasant or undesirable event**, such as a fraud or a system failure.

Risk Identification Process: Make a subjective determination about which "risks" are relevant. ("Risk" can be causes, events or effects; no restriction on overlaps; no differentiation between "risks" and "controls.")

Risk Assessment/Measurement Method: Calculate risk by multiplying likelihood and impact. (This yields the average or probability weighted severity.)

Analysis Period: Point in time analysis.

What is measured: Loss from one specific incident (severity with frequency of 1).

Focus: Day to day management of individual, **routine** issues or incidents (reactive).

Modern

Definition Risk is defined as **a measure of exposure to losses** at a specified confidence level, in excess of the mean.

Risk Identification Process: First define the "risk" universe, consisting of a finite (comprehensive) set of mutually exclusive (non-overlapping) "risk" classes. Use historical loss data to reveal where the losses (and hence the "risks") exist.

Risk Assessment/Measurement Method: Calculate risk by measuring the aggregate exposure above the mean at a specified probability level (e.g., 99%). (This yields a kind of "worst case" aggregate loss.

Analysis Period: Period of time analysis (e.g., one year).

What is measured: Aggregate loss from all incidents during one year (frequency and severity).

Focus: Management of classes of events (a portfolio view), to manage the **large** exposures using internal and external data, metrics and incentives (proactive).

The path from traditional to modern ORM.

- Adopt the modern definition of risk.
- Don’t confuse “risk types” with “control types.”
- Recognize that “identifying your risks” means establishing a pre-defined universe of risks classes and letting the data tell you where the high risks exist.
- Conduct risk assessment independently from control assessment.
- Don’t use likelihood and impact analysis for risk assessment.
- Don’t define high risk to be high likelihood and high impact.
- Don’t confuse likelihood and frequency.
- Recognize that historical loss data is the starting point for risk assessment and control assessment.
- Recognize that ORM is a process that leads to more educated decision making, which can increase profitability, not a compliance exercise.

Some recommendations for regulators.

- Provide the industry with a clear definition of the term "*risk*." Require that this definition be used in every aspect of the bank's ORM framework (not just the VaR models). Make clear that the product of likelihood and impact is not risk, nor even the expected loss.
- As part of the use test, determine whether the tail component of the expected loss is specifically incorporated into product prices.
- Educate the industry on the uses and misuses of historical loss data. Require that any use of external data be based on the objective application of data sets not the subjective manipulation of individual data points.
- As part of the Pillar III requirements, ask banks to disclose the confidence intervals around their model results, i.e., the range of expected loss and unexpected loss estimates that could be calculated by varying any weights and assumptions based on "expert judgment."

QUESTIONS & ANSWERS

When the answers are unclear…

… is it because we are asking the wrong questions?

Biographical Information – Ali Samad-Khan

Ali Samad-Khan is *President* of OpRisk Advisory. He has nearly ten years' experience in operational risk measurement and management and more than twenty years of experience in financial services.

Ali has advised more than fifty of the world's leading banks, insurance companies, energy companies, technology companies and regulators on the full range of operational risk measurement and management issues. His significant practical experience in this field comes from managing the implementation of over ten major operational risk consulting engagements at leading institutions in North America, Europe, Asia, Africa and Australia. Key elements of his framework/methodology have been adopted by numerous leading financial institutions worldwide and have also been incorporated into the Basel II regulatory guidelines.

For his pioneering work in operational risk management, Ali was named "one of the 100 most influential people in finance" by *Treasury & Risk Management* in the June 2006 edition of the magazine.

Ali has frequently advised the major bank regulatory authorities, including the Risk Management Group of Basel Committee, the Committee of European Banking Supervisors, the Board of Governors of the Federal Reserve System, the Deutsche Bundesbank, the Bank of Italy, the French Banking Commission, the Financial Services Authority (UK), the Central Bank of the Philippines, Bank Indonesia, the State Bank of Pakistan, the Bank of Thailand and the Australian Prudential Regulation Authority. He also holds seminars/workshops in North America, Europe, Asia and Australia for banks, national and international regulators and the general public.

Prior to founding OpRisk Advisory, Ali was founder and President of OpRisk Analytics LLC, which was acquired by SAS in 2003. (From June 2003 to September 2004 Ali provided transitional support for the acquisition of OpRisk Analytics, serving as SAS' Head of Global Operational Risk Strategy.) He has also worked at PricewaterhouseCoopers in New York, where he headed the Operational Risk Group within the Financial Risk Management Practice, in the Operational Risk Management Department at Bankers Trust as well at the Federal Reserve Bank of New York and the World Bank.

Ali holds a B.A. in Quantitative Economics from Stanford University and an M.B.A. in Finance from Yale University.

Articles include: "Uses and Misuses of Loss Data," with Bertrand Moncelet and Thomas Pinch, *GARP Risk Register*, May/June 2006. "Fundamental Issues in OpRisk Management," with Armin Rheinbay and Stephen Le Blevec, *OpRisk and Compliance Magazine,* February 2006. "Why COSO is Flawed," *Operational Risk Magazine*, January 2005; "Is the Size of an Operational Loss Related to Firm Size," with Jimmy Shih and Pat Medapa, *Operational Risk Magazine*, January 2000; "Measuring and Managing Operational Risk," with David Gittleson, *Global Trading*, Fourth Quarter, 1998. Working papers include: "How to Categorize Operational Losses – Applying Principals as Opposed to Rules" March 2002 and "Categorization Analysis" January 2003.