





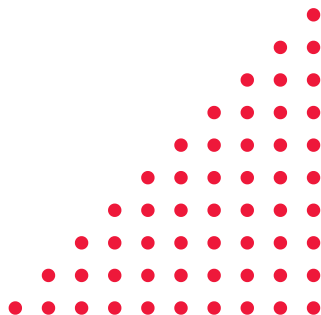
Driving Excellence in Risk and Governance

Edition 2, April 2025

✉ info@beyondriskx.com

 [BeyondRiskx](#)

 <https://beyondriskx.com/>



Editor's Note

When we set out to create the first edition of the Beyond RisX eBook, our aim was simple yet significant—to offer a practical and relatable handbook for both aspiring and seasoned risk professionals. We wanted to demystify risk management by weaving in stories from movies, references from books, and real-life case studies, while also grounding the narrative with foundational frameworks and technical insights. It was risk knowledge with a twist—digestible, engaging, and real.

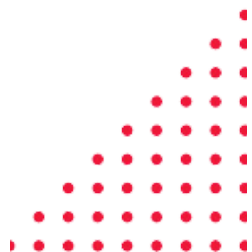
The warm reception and feedback from the community encouraged us to go further.

We are delighted to present the Second Edition of this eBook, which retains the spirit of the original while expanding its scope to cover the dynamic, complex, and fast-evolving risk landscape we are living in. This edition features a dedicated section on Emerging Risks—from geopolitical upheavals and the rise of sophisticated new-age frauds to the disruptive promise and peril of Artificial Intelligence. It also includes practical examples, such as how to design a risk taxonomy, making it even more hands-on for professionals looking to implement or enhance risk frameworks within their organizations.

At Beyond RisX, we believe risk excellence is a continuous journey. This eBook is a humble attempt to support that journey—with knowledge, with creativity, and with relevance.

We hope you find this edition insightful, thought-provoking, and above all, useful.

Warm regards,
Team Beyond RisX



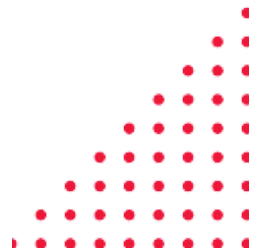
Contents

- Risk Management Basics Page 4
 - Introduction to Risk Management
 - Risk Management Frameworks
 - Key Terms used in Risk Management
 - Developing Risk Taxonomy

- Navigating Emerging Risks Page 26
 - Introduction to Emerging Risks
 - The Risk Hidden in Plain Sight
 - The Growing threat of Familiar Fraud
 - Navigating the Double Edged Sword

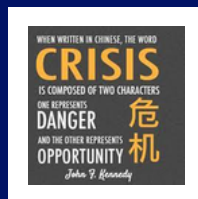
- Risk Management Careers Page 65
 - Careers in Risk Management
 - Key Skills for Existing Risk Executives
 - Professionals transitioning to Risk Management
 - Future Ready CROs

- Additional Resources Page 83
 - Risk Management Books
 - Scams and Frauds
 - Risk Management Movies



Risk Management Basics

- Introduction to Risk Management
- Risk Management Frameworks
- Key Terms used in Risk Management
- Developing Risk Taxonomy



Introduction to Risk Management

Risk Management serves as a compass, guiding businesses through uncertain waters and enabling them to navigate potential hazards with confidence, especially during these volatile times. It is crucial for everyone in the organization to be aware of their responsibilities in elevating the risk excellence culture and familiarizing themselves with essential risk management terminology which could be the difference between success and failure of an organization



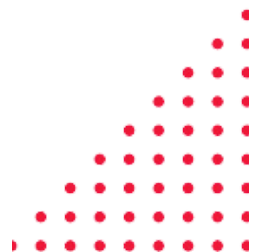
Risk Management

Risk is defined by COSO as “the possibility that events will occur and affect the achievement of strategy and business objectives.” Risks considered in this definition include those relating to all business objectives, including compliance.



Enterprise Risk Management (ERM)

"The culture, capabilities and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risks in creating, preserving and realizing value" (COSO).



Introduction to Risk Management

Operational Risk

Risk of loss due to people, processes, systems and external events. Some of the categories covered under Operational risk are Cyber and Technology risks, fraud and compliance risk .

E.g- Regulatory fines for violation of EU data privacy requirements (Meta) , Fraud (Soc Gen and JP Morgan).

Credit Risk

Risk of non- payment or underpayment of debts owed by the company. It also includes the diminution in value of debt instruments that company has invested in and hold in its investment portfolio.

E.g- Non-payment of debts extended by the Indian Banks to Gitanjali Gems, Vijay Mallya.

Market Risk

Risk of loss due to fluctuations in process of various trading items like equity, derivatives, commodities and currency.

E.g - Increasing oil prices due to Russia Ukraine conflict.



Introduction to Risk Management

Liquidity Risk

Risk of deficient cash reserves that could lead to distress sale of liquid or semi liquid assets, lowering of the credit rating of the company and in some extreme cases even bankruptcy of the company.

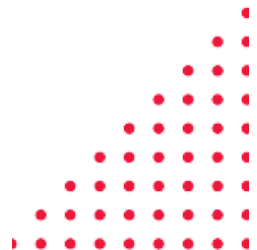
E.g- ILFS falling short of cash and defaulting on several of its obligations. Crisis at SVB (combination of Interest risk and liquidity risk).



Strategic Risk

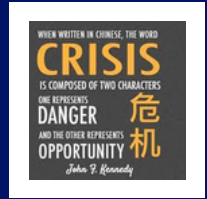
Risk of loss due to poorly conceptualized, articulated or implemented business strategy or adverse factors that result in negating the benefit of strategy .

E.g- Failure of Harley Davidson and Ford Motors (new markets) in India Nokia and Kodak (not innovating enough or recognizing the competition).



Risk Management Basics

- Introduction to Risk Management
- Risk Management Frameworks
- Key Terms used in Risk Management
- Developing Risk Taxonomy



Risk Management Frameworks

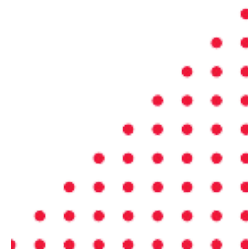
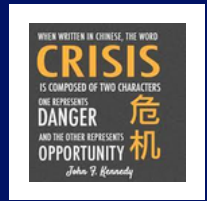
As organizations navigate an increasingly complex and interconnected business landscape, the need for effective risk management has become paramount. The Enron crisis in 2003 served as a wake up call and since then several frameworks and standards have emerged to address multitude of risks faced by organizations in today's rapidly changing environment - from COSO, ISO 31000 to NIST, TCFD and SASB.

As risk practitioners, familiarizing ourselves with various frameworks and embedding these framework as part of organization fabric provides a strong foundation to develop an effective and efficient risk program for the organization.

Here are some of the widely used risk frameworks and standards used in many organizations

Risk frameworks define the essential components, suggest a common language and provide clear guidance for development of ERM program in an organization.

Choice of the framework depends on multiple factors including the Industry in which organization is operating, business goals, organizational structure, technology infrastructure, risk category etc.



Risk Management Frameworks

COSO ERM Framework (2017)

*COSO ERM framework highlights the importance of considering risk in both strategy-setting process and in driving performance. It focuses on creating and preserving the enterprise value with emphasis on managing risks within organization's risk oversight

COSO ERM framework is used by most of the large organizations, banks and financial institutions.



ISO 31000:2018

*ISO 31000 standards, provides principles, framework and process for managing risks. It help organizations to integrate the process of managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

ISO 31000 Framework is customizable for organizations, regardless of size, industry of sector.

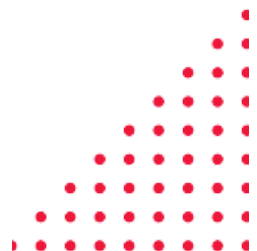


NIST

*NIST Cybersecurity framework is voluntary guidance, based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk. It helps the organizations to better integrate and align cybersecurity risk management with broader ERM process.



This is the go to framework for organizations when it comes to Cyber Security.



Risk Management Frameworks

COBIT

*COBIT is a framework created by ISACA with the goal to provide a common language for IT professionals, business executives and compliance auditors to communicate with each other about IT controls, goals, objectives and outcomes.

This framework is mainly used by organizations that operate in highly digitized environment.



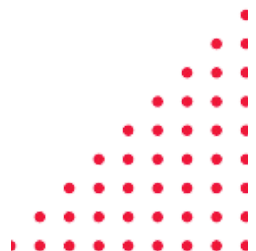
TCFD

*TCFD framework helps public companies and other organizations to disclose climate related risks and opportunities in a more consistent, transparent and effective way. It is also aimed at allowing companies to incorporate climate-related risks and opportunities into their risk management, strategic planning and decision-making processes.



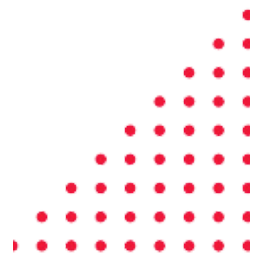
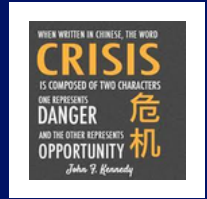
SASB

*SASB's stated mission "is to establish industry-specific disclosure standards across ESG topics that facilitate communication between companies and investors about financially material, decision-useful information."



Risk Management Basics

- Introduction to Risk Management
- Risk Management Frameworks
- Key Terms used in Risk Management
- Developing Risk Taxonomy



Risk Management Terms

Risk Assessment

"The overall process of risk identification, risk analysis and risk evaluation" (ISO Guide 73: 2009).

Horizon Scanning

"Systematic examination of information to identify potential threats, risks, emerging issues, and opportunities, allowing for better preparedness and the incorporation of mitigation into the policy-making process" (Institute of Risk Management).

Risk Identification

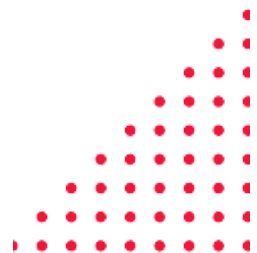
"Process of finding, recognizing and describing risks" (ISO Guide 73: 2009) This can be done through brainstorming, Internal and external surveys, horizon scanning etc.

Risk Criteria

Terms of reference against which the risks are evaluated (ISO Guide 73: 2009) This includes both quantitative and qualitative criteria like financial impact, fines and penalties, reputational harm etc.

Risk Analysis

"Process to comprehend the nature of risks and determining the level of risk" (ISO Guide 73:2009) This is done by assigning Impact and likelihood scores to the identified risks.



Risk Management Terms

Risk Matrix

Tool for ranking and displaying risks by defining range for consequences and likelihood (ISO Guide 73: 2009).



Risk Profile

Risk Profile provides a comprehensive and consolidated view of all the critical risks, across the enterprise, entity or division.



Risk Velocity

Risk Velocity is the potential speed at which the impact of the risk, if it materializes, will be felt by the organization.



Risk Treatment

"Process to modify risk" (ISO Guide 73:2009) This can be done through risk elimination, risk reduction or risk transfer. Some treatments once implemented become controls.

Risk Treatments

Eliminate	<input checked="" type="checkbox"/>
Reduction	<input type="checkbox"/>
Transfer	<input type="checkbox"/>
Retention	<input type="checkbox"/>

Controls

Measure that maintains and or modifies risks (ISO 31000: 2019).



Risk Owner and Control Owner

Risk Owner is a person or entity with accountability and authority to manage a risk (ISO Guide 73-2009) Control owner is responsible for ensuring controls activity is in place to mitigate the risk and the effectiveness of the same.



Risk Management Terms

Risk Appetite : Overall Level of risk that an organization is prepared to accept in pursuit of its objectives before it takes action deemed necessary to reduce that risk.

Risk Tolerance: Acceptable level of variation relative to achievement of a specific objective at a department, business unit or specific risk category level.

Inherent Risk: Level of risk that is naturally inherent in a process or level of risk considering no controls or other mitigating factors were in place.

Residual Risk: The level of risk, after taking into account, the effectiveness of controls and other mitigating factors.

Risk Evaluation

"Process of comparing the results of risk analysis with the risk criteria to determine whether the risk is acceptable or tolerable " (ISO Guide 73: 2009).

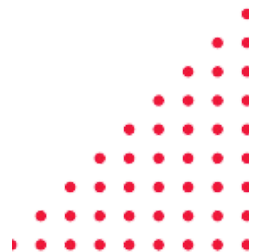
Key Risk Indicators (KRIs)

Metric or indicator used to measure and monitor the risks or unfavourable events that can adversely impact the organization's ability to achieve their objectives



Risk Management Basics

- Introduction to Risk Management
- Risk Management Frameworks
- Key Terms used in Risk Management
- Developing Risk Taxonomy



Developing Risk Taxonomy

Nishtha Khurana

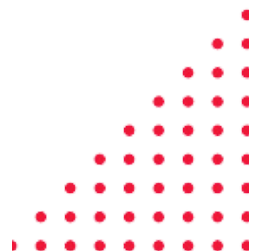
A Risk Taxonomy is a structured hierarchical classification of potential risks that may impact a company's goals or objectives. It spells out key terms and definitions used to describe risks that an organization faces and creates a common language for risk identification.

The Taxonomy breaks down risks into categories and subcategories to make them more manageable. It serves as the starting point for risk strategy, risk appetite, and risk management policies. A Risk Taxonomy seeks to establish a common language that covers business processes, risk-rating scales and standard articulation for risks and controls. It is a tool that is extremely sought after by corporates and organizations that are diversified across business products/services, geographies, legal entities etc. (for the ease of understanding, let us refer to them as 'Business Units').

Risk Taxonomy brings all different units under one risk language and make them comparable and compatible for common documentation. These organizations can use Risk Taxonomy to identify, classify, and manage different types of risks in an organized way within an organization. The steps to design and implement a Risk Taxonomy in an organization is guided very much by the general principals of Risk Management.

Whether individually, or for designing the Risk Taxonomy, the lifecycle of Risk Management remains the same. There are five phases in the risk management lifecycle, which remain constant for all levels of hierarchies of risks in a Risk Taxonomy.

A Risk Taxonomy seeks to establish a common language that covers business processes, risk-rating scales and standard articulation for risks and controls



Developing Risk Taxonomy



Unlike application of these five phases of Risk Management for each risk, in case of a Risk Taxonomy, the phases of Risk Management are applied to all levels of risk in the same sequence. Brenda Boulwood, in her article, “How to Develop an Enterprise Risk Taxonomy” provides a graphical description of the first step, i.e. agreeing on the risk categories (i.e. risk identification).

	FINANCIAL	BUSINESS	OPERATIONAL	LEGAL/REGULATORY	TECHNOLOGICAL	ENVIRONMENTAL
Risk Categories	Liquidity Market Credit	Quality of Outputs Customer Relationships Competition	Press Coverage Social Media Surveys	Human Capital Digital Processes External	Customer Behavior Technology Regulation Changes	Environmental Social Governance
Category Definitions	Ability to obtain sufficient liquidity/funding capacity	Risk of unsuccessful performance due to potential threats, actions, or events adversely affecting the ability to achieve its objectives	Potential negative publicity regarding business practices, regardless of validity	Risk of loss from inadequate or failed internal processes, people, financial reporting, systems, or external events	Risk of collapse, 3-5 year horizon	Risk of loss and associated harm due to the organization's interaction with the environment

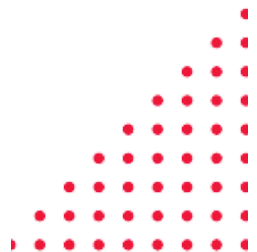
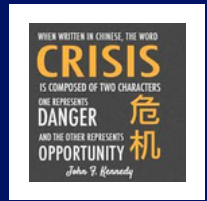
Agreeing on risk categories (i.e. level 1 risks) and mapping them to more granular risk levels (ideally leading to level 3 or level 4 of risks) is akin to identifying the risks and defining them. The Risk Taxonomy typically categorizes risks into distinct types and levels, each with a further subset with its own set of characteristics, causes, and potential impacts. It may include the following as various categories (not an exhaustive list):

The Risk Taxonomy typically categorizes risks into distinct types and levels, each with a further subset with its own set of characteristics causes, and potential impacts.



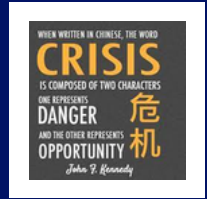
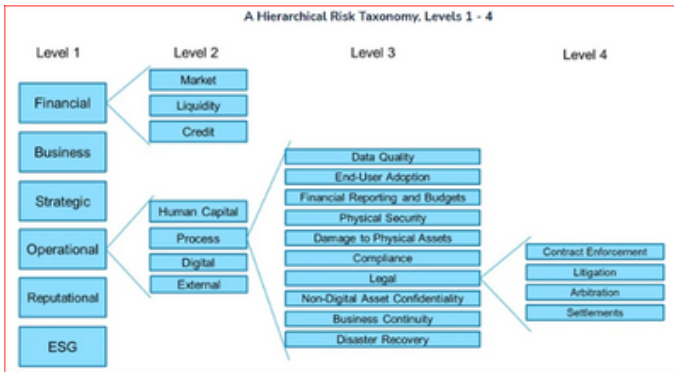
Developing Risk Taxonomy

Level 1 Risks	Description	Examples
Strategic Risks	These are risks associated with the company's strategic planning and execution.	Strategic Planning errors, lack of digital innovation, market disruptions, competition threats, etc.
Financial Risks	These risks pertain to the financial operations of the company.	Liquidity Risk, Credit Risk, Hedging Risk, Market Risk, Budget overruns, etc.
Operational Risks	These are risks associated with the day-to-day operations of the business.	Supply-chain risks, IT system failures, Cybersecurity Risks, Process deficiencies, Plant and machinery breakdowns, etc.
Reputational Risks	These are risks that could damage the reputation of the business.	Negative media coverage, Involvement in scandals, Breach of data privacy leading to exposure of customer information, etc.
Regulatory Risks	These include risks related to legal and regulatory compliance.	Lawsuits and litigation, Regulatory non-compliance, Data privacy breaches, Contractual breaches, etc.



Developing Risk Taxonomy

The same steps are then followed for identification of Level 2 Risks and so on. Brenda Boulwood graphically depicts through an example in her article, how a Level 4 Risk Taxonomy can be broken down hierarchically



Once we have the Risk Hierarchies in place, the next step would be to document all Business Units that need to be included in the Risk Taxonomy.

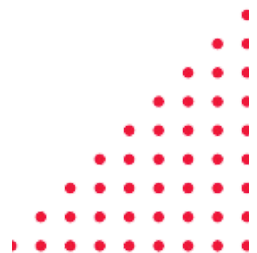
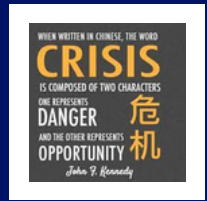


Developing Risk Taxonomy

This is usually a known metric as before the whole exercise is started, the organizations have already identified the different business corporations, subsidiaries, functions, processes / sub-processes which they would like to include to bring them on common grounds.

For example, an organization has three different business lines and may like to include all three business lines in the Risk Taxonomy. In that case, all risks identified and documented to the most granular level will then be evaluated for applicability first; and risk rating thereafter (if the risk is applicable to the business line). Similarly, an organization may like to rather evaluate risks against functions like Sales, Marketing, Operations, Finance, Human Resource etc.; and yet another organization may choose to evaluate risks against the processes / sub-processes like Job Shop Manufacturing, Batch Manufacturing, Repetitive Manufacturing, Lean Manufacturing, etc.

The next step is to pick up each granular level risk and evaluate its relevance against each business unit. For each risk, the Risk Management professionals brainstorm with relevant stakeholders and identify whether the risk is applicable to that business unit.



Developing Risk Taxonomy

The nature of a Risk Taxonomy is to standardize risk definitions for the organizations and ensure that the same language and same templates are used in all business units. However, an important corollary of this aspect is that all risks may not be applicable to all business units. Hence, the exercise to identify applicability of a risk is very important.

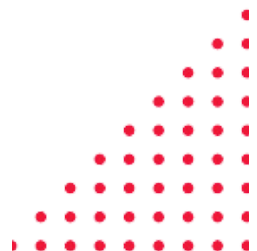
This becomes the scope of Risk Management for the Risk Management professionals. The Risk Management professionals will further proceed only for the risks in scope for their business unit. As a next step, they discuss and document all controls implemented against the risks.

This exercise is performed for every risk for every business unit and every control mapped to each risk is documented. It is by no means a miniscule exercise and great caution is required as there may not be one-to-one mapping of risks and controls. One risk can have multiple controls and similarly, one control can mitigate multiple risks.

Thereafter the Risk Taxonomy enters the next stage of Risk Management i.e. Risk Analysis or Risk Assessment. In this stage, the Risk Management professionals start the exercise of rating each risk.

Although there are many ways to assign ratings to a risk, the most commonly used tool is the impact and likelihood based Risk Rating.

However, an important corollary of this aspect is that all risks may not be applicable to all business units. Hence, the exercise to identify applicability of a risk is very important.



Developing Risk Taxonomy

An Impact-Likelihood-based Risk Rating or Risk Score is best calculated as a product of the impact of the risk materializing and the likelihood (or probability) of the risk materializing.

Brenda Boultonwood, in her article, “How to Develop an Enterprise Risk-Rating Approach”, explains that the impact and likelihood rating “allow risk heatmap graphs to simplify the communication of top risks. Moreover, within a business process or department, risk scores can be trended over time to understand the impacts of strategy, business and risk treatment investments.”

A matrix of 3x3 or 4x4 or 5x5 may be assigned to the magnitude of the risk impact and likelihood of its occurrence and its product determines the Risk Rating. A higher rating (25 being the highest in a 5x5 matrix) represents a risk with the highest possible impact and the highest likelihood of occurrence. This may be a risk that can lead to immense losses and is almost a certainty.

The Risk Ratings are assigned to risks twice. Once to measure the inherent risks, which are calculated before taking into account the controls; and the second time to score residual risks, which are calculated after taking into account the controls.

An Impact-Likelihood-based Risk Rating or Risk Score is best calculated as a product of the impact of the risk materializing and the likelihood (or probability) of the risk materializing



Developing Risk Taxonomy

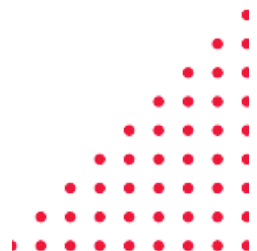
The step in between the two involves the third phase of the Risk Management lifecycle i.e. Risk Mitigation Planning. This involves assessing the effectiveness of the controls mapped against risks which helps assess how much of the inherent risks have been addressed and how much is left unaddressed.

These residual risks, in case they exceed the company's risk appetite may need strengthening or might even need additional controls to be implemented. Moreover, there may even be scenarios where the Risk Management professionals might identify Risks assessed as applicable which might not have been so identified earlier. This is a common occurrence and a wholesome risk assessment as part of developing a Risk Taxonomy is undertaken. In this case, controls need to be implemented afresh against these risks.

Then comes the fourth phase of Risk Management lifecycle – Risk Management Implementation. The controls that need to be implemented are documented as time-bound mitigation plans with action owners and due dates. These are then actioned upon, and Risk Management professionals provide oversight and advisory for the same.

Once the actions are complete, the Risk Management professionals re-perform the controls effectiveness assessment; re-calculate the residual risks; and compare the same with the Risk Appetite. Any deviation still needs to be brought to the notice of the Management and/or the Board. They may deliberate whether to re-visit the Risk Appetite; implement further controls (involving greater costs); or “accept” the residual risk beyond the appetite.

These residual risks, in case they exceed the company's risk appetite may need strengthening or might even need additional controls to be implemented.



Developing Risk Taxonomy

The last phase of the Risk Management lifecycle, Review and Tracking, is a continuous exercise of monitoring and reporting that is performed by the Risk Management professionals. In terms of a Risk Taxonomy, this usually translates to linking the Risk Taxonomy to the annual Enterprise Risk Assessment exercise. In this case, the inherent and the residual risks are plotted on a risk heatmap, usually the level 2 of Risk Hierarchy, and presented to the Management / Board, and other stakeholders (if any), which then forms basis of decision making including strategic planning.

The Risk Taxonomy is not an aim in itself, but a means to an end. Remember, the purpose of creating a Risk Taxonomy is not to capture every conceivable risk, but rather to provide a framework that can guide the organization's Risk Management efforts in a structured and systematic way. Before creating a Risk Taxonomy, it is vital to understand the business context and its objectives and strategies. Moreover, to use a Risk Taxonomy effectively, the risks identified in the Taxonomy should be translated into effective tools for managers to assess their exposure to them.

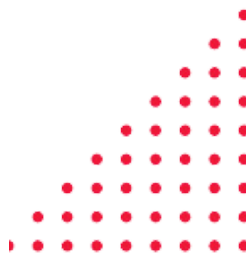
It is also worth noting that a Risk Taxonomy should not be static. It should be regularly reviewed and updated to reflect changes in the organization's internal and external environment. This ensures that the organization is always prepared for current and emerging risks. In conjunction with annual Risk Assessment, Risk Taxonomy should be periodically refreshed in an ongoing process as part of your organization's overall Risk Management Framework.

The author is Director- Control Management, in a Fortune 100 company. She is a qualified Chartered Accountant, Certified Fellow of IRM, and a Certified Independent Director. She has worked with organizations like Deloitte, RBS, Home Credit and Grant Thornton in the past. The views expressed are personal.

The purpose of creating a Risk Taxonomy is not to capture every conceivable risk, but rather to provide a framework that can guide the organization's Risk Management efforts in a structured and systematic way.

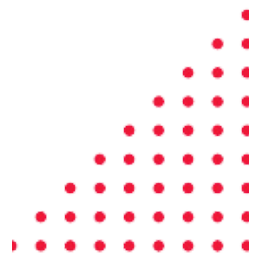
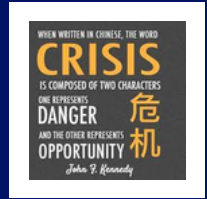


Nishtha Khurana



Navigating Emerging Risks

- Introduction to Emerging Risks
- The Risk Hidden in Plain Sight
- The Growing threat of Familiar Fraud
- Navigating the Double Edged Sword



Introduction to Emerging Risks

Risk : Risk is defined by COSO as “the possibility that events will occur and affect the achievement of strategy and business objectives.” Risks considered in this definition include those relating to all business objectives, including compliance.

Emerging Risks

“A new or unforeseen risk that we haven’t yet contemplated. This is a risk that should be on our radar, but is not, and its potential for harm or loss is not fully known”.

“A risk that is evolving in areas and ways where the body of available knowledge is weak”.

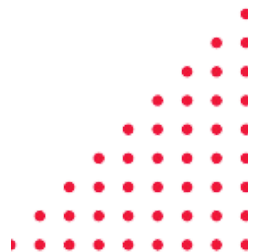
“A new risk, or a familiar risk in a new or unfamiliar context (re-emerging)”.

Characteristics of Emerging Risks :

- Driven by External Events
- Difficult to Identify and Assess
- Chaotic and Volatile
- Compound and Complex

“A new or unforeseen risk that we haven’t yet contemplated.

This is a risk that should be on our radar, but is not, and its potential for harm or loss is not fully known”.



Introduction to Emerging Risks

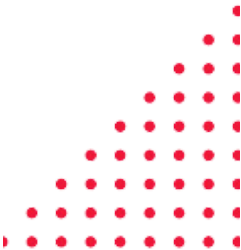
Factors Driving Emerging Risks:

We are living in unprecedented times (VUCA world) and the velocity of change in economic and business environment is at all time high. Consequently, the risk landscape is also evolving at an accelerated pace over last few years.

Factors like high cost of living, increasing interest rates, looming economic recession, climate changes, geo- political conflicts, cyber attacks and privacy risks are increasingly driving many of big risk events that have manifested in recent times

New business models, redefined customer playbooks, social trends and rapidly evolving technology are transforming competitive and industry landscape but at the same time exposing the businesses to new categories of risks or accelerating the already known risks.

New business models, redefined customer playbooks, social trends and rapidly evolving technology are exposing the businesses to new categories of risks or accelerating the already known risks.



Introduction to Emerging Risks

1. Changing Economic Environment:

- Economic downturn in and slow rate of economic growth
- High rate of Interest, Inflation, liquidity and Debt crisis
- High cost of food, fuel and other essentials impacting vulnerable sections of the society.

2. Acceleration of Innovation and Digitization:

- Innovation is happening at a faster pace.
- Pressure on revenue and use of automation and disruptive technologies.
- Consumer behavior is changing.

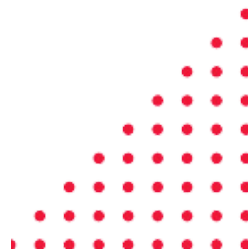
3. Geo-Political Tensions:

- New form of globalization shaping up; move towards localization.
- Concerns around security and disruptions.
- Increased focus on resiliency and efficiency.

4. Increased Focus on Environmental and Societal Factors:

- Big Push from government and regulators.
- Pressure from Investors.
- Millennial and Gen Z .
- Social media, society pressure.

Changing Economic environment, acceleration of innovation and digitization, Geo- Political tensions and Increased focus on ESG factors are some of the critical reasons contributing towards emergence of new risks.



Introduction to Emerging Risks

Key Emerging Risks:

1. Stubborn inflationary pressures, liquidity crisis, economic downturn and debt crisis at global level will bring more risks of stagnation, divergence and distress.
2. Geopolitical fragmentation will drive geoeconomics warfare and heighten the risk of multi- domain conflicts.
3. Technology will exacerbate inequalities while risks from Cyber security will remain a constant concen.
4. Climate mitigation and climate adaption efforts are setup for a risky trade-off, while nature collapses.
5. Food, fuel and cost crises exacerbate societal vulnerability while declining investments in human development erode future resilience.
6. As volatility in multiple domains grows in parallel, the risk of polycrises will accelerate.

Food, fuel and cost crises exacerbate societal vulnerability while declining investments in human development erode future resilience.



Introduction to Emerging Risks

Need to Address Emerging Risks:

While traditional risk management focuses on supporting an organization to achieve its objectives and plans, tackling emerging risks enables an organization to build and maintain resilience to ensure that it will survive and even thrive in uncertain times.

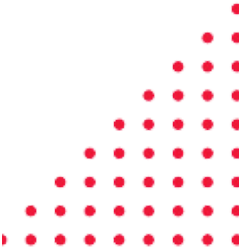
Resilience can enable the organizations to:

- Anticipate possible adverse scenarios or events, prepare for them, withstand or absorb their impacts, recover from the effects and adapt to the changing conditions.
- Respond and adapt to opportunities and take prompt and informed decisions with confidence.

Approach to Address Emerging Risks:

- Integrating Emerging risk considerations into strategic planning process (New Product Launches, Mergers & Acquisitions)
- Building risk excellence culture and fostering Innovation and agile approach
- Cross functional collaboration in risk identification and management (Tech, Cyber Security, others) groups)
- Engaging stakeholders and leveraging external insights (External suppliers. Vendors, External Data, industry body)
- Encouraging open communication and knowledge sharing.

Tackling emerging risks enables an organization to build and maintain resilience to ensure that it will survive and even thrive in uncertain times.



Introduction to Emerging Risks

Techniques to Identify Emerging Risks:

Identifying and Assessing emerging risks is a challenging tasks but there are some techniques that can help in this exercise.

1.PESTLE Analysis:

A PESTLE analysis studies the key external factors (Political, Economic, Sociological, Technological, Legal and Environmental) that influence an organization. It can be used in a range of different scenarios and can guide people professionals and senior managers in strategic decision-making.



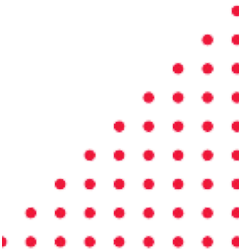
2.Horizon Scanning:

Horizon scanning is the systematic examination of potential threats, opportunities and likely future developments which are at the margins of current thinking and planning' and, continuing, horizon scanning 'may explore novel and unexpected issues, as well as persistent problems or trends.



3.SWOT Analysis:

SWOT analysis is a framework for identifying and analyzing an organization's strengths, weaknesses, opportunities and threats. The primary goal of SWOT analysis is to increase awareness of the factors that go into making a business decision or establishing a business strategy.

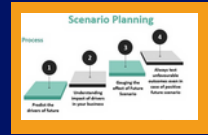


Introduction to Emerging Risks

Scenario Planning and Stress Testing:

Scenario planning helps decision-makers identify ranges of potential outcomes and impacts, evaluate responses and manage for both positive and negative possibilities. By visualizing potential risks and opportunities, businesses can become proactive versus simply reacting to events.

Stress testing is a form of deliberately intense or thorough testing, used to determine the stability of a given system, critical infrastructure or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.



Introduction to Emerging Risks

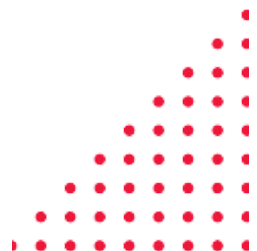
Mitigating and Resilience Strategies:

- Agile and Timely Response
- Leverage Technology
- Build Long Term Resiliency
- Learn and Adapt

Latest Trends in Risk Management:

- **Strategic Integration:** Integrating risk management factors into key strategic objectives including focusing on ESG, Automation, Transformation and Digitization.
- **Pervasive Controls:** Developing and implementing controls that are more pervasive as organizations become more inter-connected and digitized.
- **Analytics:** Using data and technology to identify key themes, trends and leading indicators including predictive modelling.
- **Monitoring:** Investment in detection and monitoring tools is increasing.
- **Technology:** Technology including Cognitive tools, AI, ML and Big data is being used more widely.

Agile and timely response and adapting quickly are some of strategies to mitigate emerging risks



Introduction to Emerging Risks

Role of The Board:

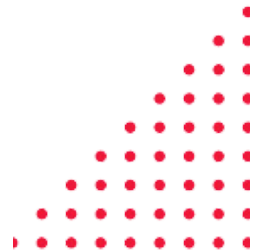
Some boards view risks as "black swans" (hard to predict and very impactful – such as the COVID-19 pandemic or the global financial crisis of 2008). However, highly resilient boards gain an advantage by also leaning into the concept of risks as known unknowns, i.e., gray rhinos, and they change their behavior in the face of these risks.

1.Informed confidence: Highly resilient boards know management has the right systems, processes and governance frameworks in place to scan the horizon and detect known, emerging and interconnected risks – and understand how they will impact strategic business objectives.

2.Agility: These boards take a highly discerning and cautious view on their organization's level of preparedness to respond to these interconnected and ever-changing risks. They ask "what if" questions to challenge groupthink and confirmation bias.

3.Humility: Highly resilient boards accept that both they and their organization need to continually update their skill set to ensure they keep an eye on the horizon while management has an eye on the ground in front of them.

Highly resilient boards gain an advantage by also leaning into the concept of risks.



Introduction to Emerging Risks

Key Takeaways:

The world is witnessing set of risks that are both new e.g risk posed due to technology including cyber risk, and emergence of generative AI and climate risks, and re-emergence of old risks- like inflation, liquidity crisis geopolitical confrontation and unsustainable level of debts.

Not only these risks are causing big impact, but combination of these risks are creating polycrises situation that is evident in the way the recent events unfolded with fall of Silicon Valley bank and other similar cases.

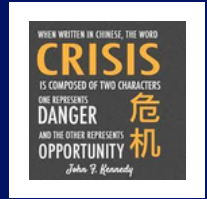
All of us have a big role to play in working with Board, Senior Management and Business Leaders in not only helping them manage through these turbulent times but also to ensure that they are proactively partnering to identify the emerging risk trends and actively address the known risks.

The world is witnessing set of risks that are both new risks and re-emergence of old risks and all of us have a big role to play in working with the Board and Senior management to help them manage through these turbulent times.



Navigating Emerging Risks

- Introduction to Emerging Risks
- The Risk Hidden in Plain Sight
- The Growing threat of Familiar Fraud
- Navigating the Double Edged Sword



Risk Hidden In Plain Sight

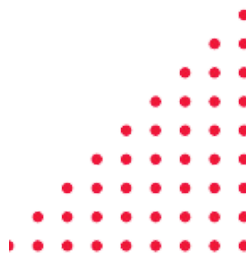
Maj General Neeraj Bali, SM (Retd)

On 7 October, during the Sabbath, Hamas militants launched an audacious attack against Israeli army posts and civilian settlements in Southern Israel. The operation, called Al-Aqsa Flood, was unprecedented in scale and ambition – and for the surprise it achieved. 1,200 Israeli and foreign nationals died, some enjoying a music festival, and 240 were taken hostage. The Hamas Nukhba ('elite commandos') captured an area of 4-5 kilometres deep and, in places, penetrated well beyond that.

How did Israel, a country known for one of the finest intelligence apparatuses (including the feared domestic intelligence agency Shin Bet) in the world and the highly-rated military, fail to unravel the risk of a Palestinian attack of this ferocity? Did Hamas manage to camouflage its plans and intent? Or was the risk hidden in plain sight, and Israel dropped the ball? What can the rest of us, particularly in the business world, learn from this unmitigated fiasco that has resulted in a year-long bloodletting and severe geopolitical impact?

We now know that Hamas gathered information about the Israeli defences – the hi-tech fence backed by sensors and towers – over a long time. It also meticulously studied the routes and direction of the Israeli Defence Forces (IDF) reaction to provocations. Workers from Gaza, who Israel permitted to enter daily, were one possible source of this information.

How did Israel, a country known for one of the finest intelligence apparatuses (including the feared domestic intelligence agency Shin Bet) in the world and the highly-rated military, fail to unravel the risk of a Palestinian attack of this ferocity?



Risk Hidden In Plain Sight

Within its rank and file, Hamas maintained strict control of information and the assaulting militants were briefed about targets only on the morning of the attack. The pattern of equipping these militants indicates that there was every intention to stay for a long time.

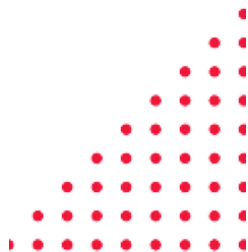
The plan worked perfectly. Using drones laden with explosives, the infiltrators neutralised the communication systems and sensors. The surveillance posts, too, were attacked. The control stations meant to piece together the emerging picture, were blinded. Other militants landed at strategic points by using motorised paragliders, poised to block any reinforcements. The fence was breached by militants moving on foot, motorcycles, bulldozers and trucks. This mayhem was backed by a barrage of over 2,500 rockets, targeting areas even as deep as Tel Aviv and Jerusalem.

What were the reasons for failing to discern the risk and meet the challenge it reared? More importantly for us, what are the lessons that the corporate can draw?

Disregarding Sources of Information

Intelligence units of predominantly women operatives manned sections of the Israeli border where the attack materialised. These professionals had noticed specific changes in the pattern and behaviour of the movements. Indeed, even information on the suspicion of Hamas fighters rehearsing attacks was also relayed to commanders. It is widely believed within Israel that the reason these inputs were ignored was because women operatives were not considered as competent as their male counterparts. Indeed, 'male chauvinism' appears to have been a cause. Ironically, some of the very women soldiers who had given accurate inputs ended up being hostages or getting killed.

What were the reasons for failing to discern the risk and meet the challenge it reared? More importantly for us, what are the lessons that the corporate can draw?



Risk Hidden In Plain Sight

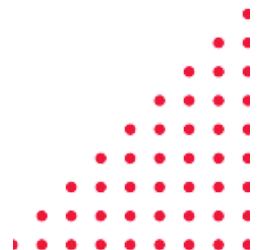
The lesson is not only about eliminating gender bias while evaluating sources. A large retailer deciding to enter a new market by researching only well-established consulting reports may miss emerging trends or smaller but more insightful local data sources. Establishing a process that evaluates all sources—regardless of origin—on merit is crucial. Salespersons in contact with market realities and potential clients must be integrated into the ‘information gathering’ system.

Lesson: input must be evaluated based on process and merit, not on the provider's perceived background or preconceived notions.

‘Groupthink’ can become the Enemy of Risk Analysis. Israel believed that Hamas no longer wanted to pursue a violent course but was focused on governance. Also, the threat from Hezbollah was considered more acute. This groupthink lulled Israeli civilian and military leadership, which was focused on targeting Hezbollah (the pager and mobile attacks were in the works at this point).

Similarly, Kodak's collapse is often attributed to "groupthink." The company stuck to traditional photography because the leadership couldn't escape the collective belief that digital wouldn't catch on.

Lesson: input must be evaluated based on process and merit, not on the provider's perceived background or preconceived notions.



Risk Hidden In Plain Sight

Fostering diverse perspectives in the company is the way to combat the tendency for groupthink. As hard as it is, mid- and senior leadership should be encouraged to challenge the status quo. I have a soft corner for well-intentioned mavericks whose manner sometimes dissuades leaders from listening to their counsel.

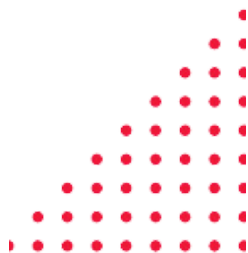
Seduced by Own Rationality!

Israeli senior officers ignored stark warning as 'fantasy'. Even a 40-page report called Jericho Wall was ignored. Warnings from Egypt were ignored as crying wolf. What led to this self-blindsiding? In assessing its risks vis a vis its multiple enemies, the Israeli leadership imposed its rationality on how Hamas would think. Since Hamas was essentially 'behaving' and appeared consumed by the desire to govern, it was deduced that it had given up the path of violence for the foreseeable future.

The Indian Army similarly faltered in analysing the risks posed by Pakistan in the months leading up to the Kargil War. It was known that there was a logistics build-up across the Line of Control. Still, our rationality dictated that since no one launches attacks in winter and the Pakistani modus operandi is to infiltrate terrorists in small groups to create trouble in the hinterland, that was the course Pakistan would take. In this instance, the enemy followed a third option of infiltrating to occupy unheld positions!

Similarly, say, the U.S. electronics industry underestimated Xiaomi's ability to thrive on thin margins, thinking it was irrational. Xiaomi's business model worked in different economic and cultural contexts.

Similarly, Kodak's collapse is often attributed to "groupthink." The company stuck to traditional photography because the leadership couldn't escape the collective belief that digital wouldn't catch on.



Risk Hidden In Plain Sight

To analyse risks, especially those related to competitors, we must know that understanding competitors' decisions requires stepping out of one's assumptions about what is "rational" or "normal" behaviour in one's context.

Even on the clearest of days, risks are hard to predict. But if we begin to see through the prism – or template – of only our rationality, we may end up misreading the big picture entirely

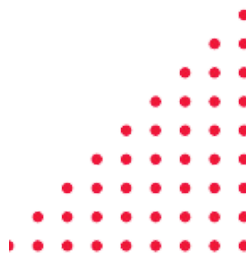
Over-reliance on Technology

Israel is known for cutting-edge technology, especially in defence-related weapons and equipment. Arguably, an overreliance on technology by intelligence agencies was partially responsible for the failure to detect the Hamas attack on October 7.

Israel's high-tech \$ 850 million 65-km over-ground and naval border barrier, replete with radar systems and command and control rooms, hundreds of cameras, radar and other sensors, is an exemplary "smart fence". It has means to detect infiltration by sea and a remote-controlled weapons system.

Hamas' planning recognised that remote-controlled sensors were vulnerable to attack by relatively simple means, such as explosive devices or hand grenades dropped from small drones.

To analyse risks, especially those related to competitors, we must know that understanding competitors' decisions requires stepping out of one's assumptions about what is "rational" or "normal" behaviour in one's context.



Risk Hidden in Plain Slight

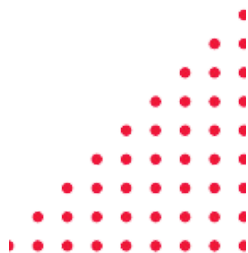
Israel also relied on intelligence from satellites, aircraft, drones, and other sensor-equipped platforms. But when it came to understanding the risk lurking next door, Israel suffered from the same infirmity that some businesses could—overreliance on technology, leading to humongous data indistinguishable from noise: the sensors, radars, and all the led-to holes in intelligence. The invasion became a reality once these were overwhelmed (including the celebrated Iron Dome).

Admittedly, technology is not the problem by itself; it is the failure to create systems to sift the streams of data—often competing signals—that technology brings us.

In the business world, a company using advanced analytics to track competitor pricing without manual cross-checks may miss nuanced changes in product quality or shifts in consumer preferences that technology cannot capture. Over-reliance on tech tools like algorithms can overlook human elements such as consumer sentiment or cultural factors, opening the doors to business risks.

When the healthcare sector started using Big Data to track patient outcomes, companies without solid analysis structures often drowned in irrelevant data, missing the essential insights that could lead to new business models. Successful pharmaceutical companies leverage relationships with healthcare professionals and scientists to understand emerging medical technologies and treatment preferences.

Admittedly, technology is not the problem by itself; it is the failure to create systems to sift the streams of data—often competing signals—that technology brings us.



Risk Hidden in Plain Slight

The lesson is to create well-structured processes and systems that capture essential information and avoid being swamped by non-critical data. While every means of technology may be used, eventually, human intervention is a must to draw the correct deductions. Manual (human) inputs, such as insights from employees or industry insiders, can often give you qualitative information that data alone can't provide.

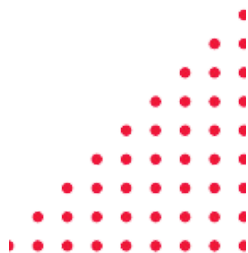
Learn to Read the Patterns Well

While Israel failed to read patterns in the changing behaviour of Hamas and Palestinians coming across the border for work, Hamas read the Israeli patterns of reinforcements and movements well. While studying risks, sometimes we are so enamoured by historical precedents and linear explanations that we miss reading meanings into emerging patterns.

Predictable patterns are recurring trends or behaviours in data, markets, or operations that can be anticipated based on historical information or consistent factors. These patterns often indicate potential risks or opportunities. For a risk analyst, spotting these patterns is a "low-hanging fruit" because patterns can usually be identified using readily available data and tools, and these trends can lead to immediate interventions that mitigate risks or leverage opportunities.

As a simplistic example, think of a company in the retail sector. A predictable pattern might be seasonal sales fluctuations, a rise during the festival season, and a marked dip in revenue during the summer months. These patterns will shadow cash flow issues, overstocking, or underperformance during summer.

The lesson is to create well-structured processes and systems that capture essential information and avoid being swamped by non-critical data.



Risk Hidden in Plain Slight

By reading this predictable pattern, the company can adjust inventory levels, launch targeted marketing campaigns, or implement sales promotions in advance. On a larger scale, Amazon's strategic acquisition of Whole Foods was based on recognising patterns in consumer behaviour, indicating a shift towards healthy, organic foods and e-commerce integration with offline channels.

The lesson is not to ignore patterns because these are business as usual. This low-hanging fruit can prevent potential financial losses and build a foundation for more profound, more complex risk assessments.

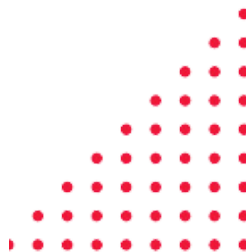
The initial success of Hamas shook Israel and surprised the world, showing us how not to assess and predict risks. Warren Buffet says, "Risk comes from not knowing what you're doing." This is especially true in asymmetric situations where a 'weaker' player will likely adopt dramatically new competitive approaches. Understanding and analysing risks in such conditions is critical to informed decision-making.

The author is an Army veteran, an ex-CEO of two companies and a management advisor. He is the author of "The Winning Culture – Lessons from the Indian Army to Transform Your Business". He is a teaching faculty member of the Institute for Competitive Intelligence, Germany, School of Inspirational Leadership, Pune and Director of the Gyan Chakra Think Tank. The views expressed are his own.

The lesson is not to ignore patterns. This low-hanging fruit can prevent potential financial losses and build a foundation for more profound, more complex risk assessments.

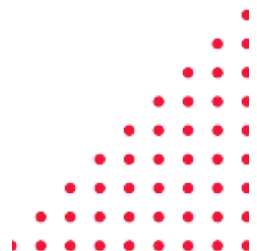
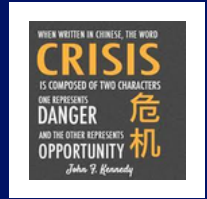


**Maj Gen. Neeraj Bali, SM
(Retd)**



Navigating Emerging Risks

- Introduction to Emerging Risks
- The Risk Hidden in Plain Sight
- The Growing threat of Familiar Fraud
- Navigating the Double Edged Sword



The Growing Threat of Familiar Fraud

Dr. Aneish Kumar

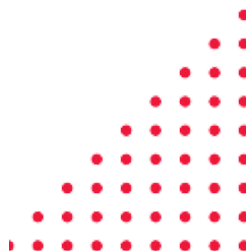
In today's digitally connected world, the threat of familiar fraud committed by someone known to the victim - is rapidly increasing. This type of fraud is particularly harmful because it involves a betrayal of trust. Fraudsters take advantage of their relationship with the victim to gain access to sensitive personal details like passwords, answers to security questions, or even physical access to devices such as smartphones or laptops. This inside knowledge allows them to bypass traditional security measures, making it difficult for financial institutions to detect irregular activity.

What's especially concerning is that familiar fraud often goes unnoticed for long periods. Since the fraudster is familiar with the victim's habits, spending patterns, and behaviours, the fraudulent transactions appear normal to detection systems. As a result, fraudsters can go on for weeks or months without raising any red flags. Even with advanced technologies like document verification, these crimes often slip through the cracks, highlighting the need for liveness detection and biometric authentication as additional layers of security.

Manipulating human emotions in cybercrime

A key element of familiar fraud—and many other types of scams—is the use of social engineering, where fraudsters manipulate human emotions such as fear, curiosity, sympathy, or pride to trick their victims. As Donna Mattingly, corporate security education expert at Mastercard, points out, "Cybercriminals often rely on human emotion like fear, curiosity, sympathy, or pride to trick their victims."

Since the fraudster is familiar with the victim's habits, spending patterns, and behaviours, the fraudulent transactions appear normal to detection systems. As a result, fraudsters can go on for weeks or months without raising any red flags.



The Growing Threat of Familiar Fraud

One striking example occurred during the COVID-19 pandemic when fraudsters exploited people's anxieties. Relatives of individuals hospitalized with COVID were contacted by scammers, posing as hospital staff, demanding urgent payments for medical bills. Driven by fear and confusion, family members often complied without verifying the authenticity of the call.

One notable example occurred in Hong Kong, where a multinational financial company lost \$25.6 million in a deepfake scam. An employee was fooled into transferring corporate funds after participating in a deepfake video call that appeared to feature the company's CFO and other colleagues. These impersonators were actually AI-generated, proving that even trained professionals can be tricked by these highly convincing tactics

These techniques are becoming even more advanced with the integration of generative AI. Fraudsters are now capable of creating highly convincing fake websites, elaborate false identities, and even AI-powered deepfakes. These deepfakes can mimic the voices or appearances of trusted colleagues, family members, or high-ranking officials, making it incredibly difficult for victims to recognize the scam.

These techniques are becoming even more advanced with the integration of generative AI. Fraudsters are now capable of creating highly convincing fake websites, elaborate false identities, and even AI-powered deepfakes.



The Growing Threat of Familiar Fraud

How fraudsters research their targets

In the past, fraudsters often relied on luck or pure opportunism. Today, however, they are far more strategic, dedicating extensive time to researching their targets. Modern cybercriminals meticulously scour social media profiles, business websites, and publicly available documents to build comprehensive profiles of their victims. Some fraudsters even subscribe to company newsletters or follow industry-specific blogs to better understand the working environments and personal habits of their targets.

Take the case of Nikki, an investment banker who became the victim of a phishing scam. Over the course of several months, a fraudster built a detailed profile of Nikki using her LinkedIn activity and other online sources. Armed with this information, the fraudster crafted an email that appeared to be from one of Nikki's clients, asking for sensitive financial details. The email was so meticulously constructed that Nikki didn't hesitate to provide the requested information, unknowingly handing over her banking credentials to the fraudster.

This level of preparation allows fraudsters to tailor their attacks to their victims, increasing the likelihood of success. In many cases, they spend weeks or even months gathering details before launching an attack, ensuring their phishing attempts are not only believable but also difficult for victims to detect.

Some fraudsters even subscribe to company newsletters or follow industry-specific blogs to better understand the working environments and personal habits of their targets.



The Growing Threat of Familiar Fraud

Tactics behind fraudulent attacks

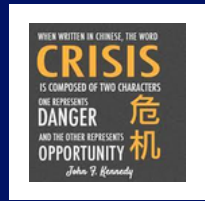
Every fraudulent attack follows a predictable pattern, beginning with research and ending with execution. Fraudsters break down their attacks into three key phases:

1. Research: Fraudsters gather as much information as possible from social media, public databases, and other online platforms. This enables them to build a detailed profile of their target.

2. Profiling: With the gathered data, fraudsters assess their target's vulnerabilities. For instance, if the victim frequently travels, the fraudster may create a fake airline confirmation email. If the target often interacts with banking systems, a phishing email disguised as a bank request might follow

3. Execution: Once the profile is complete, the fraudster launches the attack. This often involves sending phishing emails, SMS messages, or phone calls designed to impersonate trusted contacts. The goal is to trick the victim into sharing sensitive information or transferring money.

In one particularly damaging case, a large healthcare organisation fell victim to a spear-phishing attack. Fraudsters spent weeks studying the company's email patterns before impersonating the CEO in an email to the finance department. The email requested a large sum of money be transferred to a "new vendor." The finance team, believing the email to be legitimate, authorised the transfer, resulting in significant financial loss.



The Growing Threat of Familiar Fraud

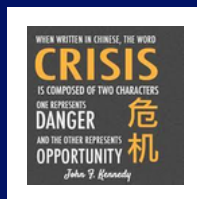
How fraudsters hide their tracks

Once they have successfully defrauded their target, fraudsters move quickly to cover their tracks. One common technique is using VPNs or proxies to mask their location, making it appear as if they are operating from another country or region.

Additionally, many fraudsters use money mules - individuals who help launder stolen funds by moving them between multiple accounts -to further obscure their involvement.

A well-known case involving a global retail brand illustrated how fraudsters launder money using multiple offshore accounts and cryptocurrencies. After gaining access to the company's financial accounts, the fraudsters quickly transferred the stolen funds across various jurisdictions and converted the money into cryptocurrency. By the time the fraud was discovered, the digital trail had gone cold, making it nearly impossible for investigators to trace the transactions.

Some more sophisticated fraudsters even go as far as deleting phishing emails from their victim's inbox or changing account settings to reroute notifications to their own devices. These actions give them more time to continue their fraudulent activities before the victim realizes something is wrong.



The Growing Threat of Familiar Fraud

The rise of AI-powered fraud

One of the most alarming trends in cybercrime is the rise of AI-powered fraud. Fraudsters now use AI and machine learning to automate much of their research, increasing both the scale and sophistication of their attacks. AI can quickly analyse social media profiles and other online data to identify potential victims, while AI-powered tools can generate highly personalized phishing emails that are difficult to distinguish from legitimate communications.

AI-powered voice cloning technology has also emerged as a significant threat. In one case, fraudsters used AI to clone a CEO's voice, calling the company's finance department to authorize a fraudulent money transfer. The cloned voice was so accurate that the finance team did not hesitate to comply, leading to substantial financial losses.

What can you do to protect yourself?

As scams become more sophisticated, protecting yourself requires greater vigilance. Here are a few practical steps you can take:

1. Minimize Your Digital Footprint: Be mindful of the information you share online, especially on social media platforms. Fraudsters often piece together small bits of publicly available information to create a detailed profile and launch tailored attacks.

One of the most alarming trends in cybercrime is the rise of AI-powered fraud. Fraudsters now use AI and machine learning to automate much of their research, increasing both the scale and sophistication of their attacks.



The Growing Threat of Familiar Fraud

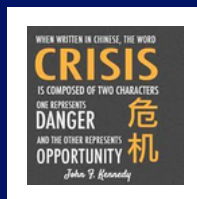
2. Use Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring additional verification, such as a code sent to your phone, in addition to your password. This makes it much more difficult for fraudsters to gain access to your accounts, even if they have your password.

3. Verify Communication Sources: If you receive a request for sensitive information via email, SMS, or phone, always verify the source before responding. Contact the organization directly through official channels to confirm the legitimacy of the request.

The role of financial institutions

Financial institutions play a crucial role in preventing fraud. As fraudsters become more skilled at using AI and Big Data, banks and financial service providers must also adopt advanced tools to protect their customers. AI-driven algorithms can analyse transaction patterns in real-time, flagging suspicious activity, while behavioural biometrics can detect deviations in user behaviour, such as changes in typing speed or navigation patterns.

Education is equally important. Financial institutions should invest in ongoing training and awareness campaigns to help customers recognize and avoid potential scams. One successful example of this is JPMorgan Chase's cybersecurity awareness program, which provides customers with resources for detecting phishing emails and phone scams



The Growing Threat of Familiar Fraud

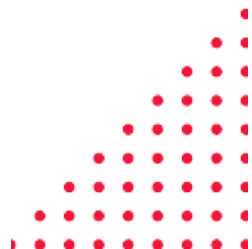
The future of fraud prevention

To prevent familiar fraud in this increasingly digital landscape, both individuals and financial institutions must adopt more sophisticated security measures. Biometric authentication and multi-factor authentication are becoming essential tools for safeguarding personal and financial data.

Additionally, financial institutions should educate their customers about the risks posed by deepfakes and social engineering. It's crucial to raise awareness that even familiar faces and voices may not be what they seem, especially when it comes to sensitive transactions.

In the long term, the future of fraud prevention will likely involve the adoption of behavioral biometrics, which analyses user behavior to identify anomalies and detect potential fraud before it occurs. Blockchain technology also holds promise as a means of preventing fraud, offering a secure, decentralized ledger that is difficult to manipulate. When combined with real-time AI monitoring, these tools could revolutionize the way fraud is detected and prevented.

The future of fraud prevention will likely involve the adoption of behavioral biometrics, which analyses user behavior to identify anomalies and detect potential fraud before it occurs.



The Growing Threat of Familiar Fraud

Conclusion

The growing sophistication of fraud- particularly familiar fraud- is a significant concern in today's digital age. Cybercriminals are no longer opportunistic; they are highly strategic, using advanced tools such as AI, machine learning, and social engineering to exploit human vulnerabilities. Whether through deepfake technology or traditional phishing tactics, everyone is at risk.

However, by staying vigilant, minimising your digital footprint, and using advanced security measures such as MFA and behavioural biometrics, you can better protect yourself from falling victim to these scams. Financial institutions must also remain at the forefront of innovation, investing in cutting-edge technology to stay ahead of increasingly sophisticated cybercriminals.

Ultimately, awareness, skepticism, and proactive security practices remain the most effective defence against familiar fraud. Staying informed and cautious ensures that even as fraudsters evolve, we remain one step ahead

The author is ex MD and Country Head of BNY Mellon, India. He currently serves on the Boards of various companies as Independent Director and Strategic Advisor. He is prolific writer and speaker on variety of subject including, Risk Management, Corporate Governance, Technology and Leadership. The views expressed are his own.



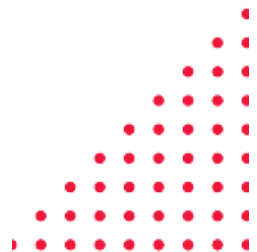
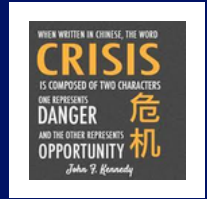
Dr. Aneish Kumar

By staying vigilant, minimizing your digital footprint, and using advanced security measures you can better protect yourself.



Navigating Emerging Risks

- Introduction to Emerging Risks
- The Risk Hidden in Plain Sight
- The Growing threat of Familiar Fraud
- Navigating the Double Edged Sword



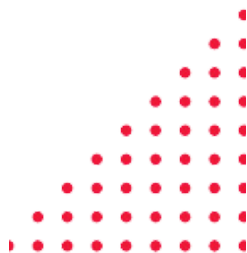
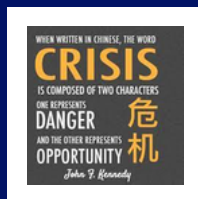
Navigating the Double Edged Sword

Veena Jadhav

Imagine this: As a routine you intend to check on traffic before leaving to work. As soon as you open the app, it knows your current location, the usual route you take, end destination and even the time you typically leave home without you telling it anything. Then, out of the blue, there's a notification that can apparently see the future and starts warning about a certain traffic congestion that might occur and suggests an alternate route. The app has made your morning a bit easier, and you feel relieved.

On the same lines, your fitness tracker tracks your steps and encourages you to stay active; as you order your food, the app suggests based on your past choices; as you scroll through social media feed, it suggests the events that's matches your thoughts; as you browse internet, the site can anticipate your demand and servers your search; All of this appears to be a bit magical, right? As if these digital assistants are always one step ahead, anticipating our requirements.

But wait a second—let's shift gears and dig a little deeper, this magic comes at a cost. While these tools make life easier and more personalized, they also carry risks we shouldn't overlook. For instance, that handy traffic app not only helps you navigate but also keeps track of your travel habits, raising concerns about your privacy. Your location, preferences, and even the routes you frequently travel are quickly recognized by your smartphone when you pick it up to check the weather. This sense of convenience can sometimes blur the line between helpful and intrusive, making it essential for us to think carefully about the trade-offs we make in our increasingly tech-driven lives.



Navigating the Double Edged Sword

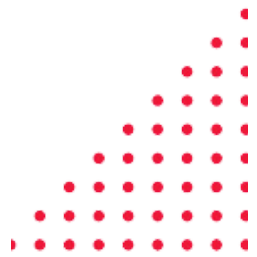
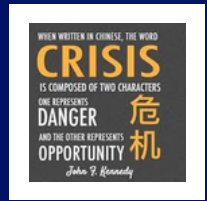
The Foundation: Understanding AI and ML

Entering the world of Artificial Intelligence (AI) and (Machine learning) seems like coming to a place which is a fusion of a compass and a mystery. The evolution of AI & ML are interweaved, both representing/mirroring aspects of human intelligence. They have the potential to enhance decision making ability basis data to optimize the processes.

These technologies definitely have been built to serve a purpose by enriching us and making us see the different sides of the same coin, but, in the very process they also prompt us to re-evaluate our perspective. Predictions, complex systems and assisting our decision making process is definitely something AI can do for us but it is also critical to note that the information it works on can be equally biased and cock-eyed as its developers.

Within the domain of risk management, the focus should be on comprehending the potential benefits as well as the challenges associated with these technologies. These technologies are quintessential tools that guide us, revealing new paths—yet they challenge our understanding at every turn.

We also have to admit that these benefits frequently come at a cost because there is no such thing as a cost-free technological convenience. This kind of understanding is what empowers us to make sound and rational use of these technologies. In this field, every shortcut, every automated insight, comes with a trade-off—and recognizing these trade-offs is where true expertise begins.



Navigating the Double Edged Sword

The Upside: Embracing the Rewards of AI and ML

Let's explore the benefits that AI and ML will bring to everyone's work, regardless of their levels in career.
The Edge of Strategy: Unlocking True Advantage.

In today's ever-evolving world, AI/ML enables organizations to identify threats and take quick action. With the help of these cutting-edge resources, experts are starting to anticipate problems rather than merely responding to them, which is a novel approach in risk domain. For example, a recent study by Deloitte shows businesses using AI for risk management are responding swiftly to emerging threats as they can detect anomalies proactively in real time.

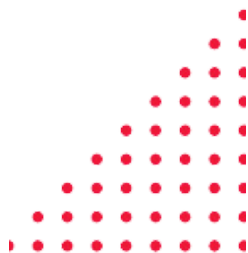
Personalization and Innovation: Crafting the Future.

Consider how AI can notice trends that humans might overlook, whether it's analyzing customer behavior or detecting red flags before they escalate. It brings in a whole new level of innovation, making the complicated apparent and providing accuracy that might feel like a leap ahead. For example, according to Boston Consulting Group (BCG,) AI enables financial institutions to customize insurance products by examining individual consumer data in sectors like bancassurance.

Efficiency and Insight: A Path to Mastery.

Imagine how simple and easy it could be to view risk assessments completed in minutes with the information of several millions of data at the click of a button. Mundane activities which would have taken days to complete are done in few hours, enabling you to devote time and energy to strategies better. For example, AI technologies are being used by financial organizations to expedite regulatory reporting procedures so that risk managers may concentrate on higher-value tasks as per Deloitte's study.

In today's ever-evolving world, AI/ML enables organizations to identify threats and take quick action. With the help of these cutting-edge resources, experts are starting to anticipate problems rather than merely responding to them.



Navigating the Double Edged Sword

In risk management, AI and ML aren't just tools—they're a way to anticipate and prevent issues before they emerge. For newcomers, they offer a first look at cutting-edge capabilities; for experienced professionals, they enhance precision and deepen insights, elevating the entire field. This shift brings risk management beyond mere reaction, opening a new era of proactive strategy and foresight.

The Dark Side: Risks of AI and ML

Nevertheless, by the virtue of being risk experts, it is acknowledged that, where there is opportunity; there is vulnerability. The term AI & ML can easily become a double edged sword!

Data Privacy Dilemmas: Who's Holding Your Secrets?

How often do you click "accept" without reading the fine print? Have you ever given any thought to where all that personal data about you may wind up? We quickly give away our personal information, including our address, preferences, and even location, without hesitation as we pursue convenience driven by AI. Our data, however, is not only saved behind these displays; it is constantly being moved, examined and frequently shared. We have little influence over how information is used since every detail we give up, adds to a complete profile that is compiled in databases that are well out of our reach.

In risk management, AI and ML aren't just tools—they're a way to anticipate and prevent issues before they emerge.



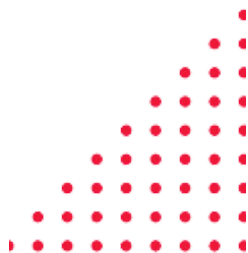
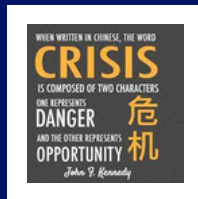
Navigating the Double Edged Sword

Let's consider a scenario: A fitness app diligently tracks your every step and heartbeat. This data, seemingly harmless, when shared with third parties, can create a detailed portrait of your identity and daily routines. So, who truly controls the access to your personal life, and how secure is it? It's essential to question whether we're comfortable trading our privacy for these 'personalized' services, or if there's a safer path, one that doesn't put our sense of security at risk for the sake of convenience.

Bias and Fairness Issues: When Technology Echoes Prejudices.

It has been established that AI & ML are to "learn" from past information, and if that information is incorrect, the outputs will equally be incorrect.

Think about a platform for job applications that inadvertently excludes some groups from employment suggestions. Another example, consider an AI loan approval system that routinely selects certain applicants above others based on "learned" patterns from biased data rather than personal quality. These are not exaggerated examples; they are becoming increasingly true. This is intriguing to seasoned risk professionals because, perhaps unintentionally, the pursuit of neutrality can result in unwarranted prejudice.



Navigating the Double Edged Sword

Cyber threats / Security Risks: Trusting the Machines We Rely On.

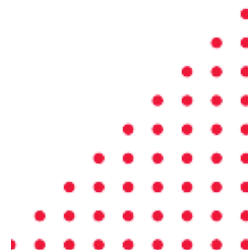
How frequently do we think about how susceptible our AI-powered gadgets may be to manipulation? As AI becomes more sophisticated, so do those who aim to take advantage of it. Customized phishing emails, incredibly realistic impersonations, and even "Deepfake" movies are examples of more complex AI-powered schemes. It's possible that an algorithm is collecting and modifying data in the background to take advantage of our trust every time you receive an email that looks uncannily tailored.

Are these systems truly reliable? It's about having control over our own digital life, not simply about being a good impersonator. It is the potential for these machines that we depend on to be the same ones that deceive us.

Reliability and Decision-Making: When Machines Fail Us.

Even while AI and ML have amazing potential, they are far from foolproof. We've all heard voice assistants misinterpret basic requests or navigation applications take us down odd paths. Even if they are inconvenient, these mistakes serve as a warning of AI's limited and even dangerous dependability. Consider a hospital that uses an AI-powered diagnostic tool that makes the incorrect advice due to a little data inaccuracy or a business automated trading system that causes a financial miscalculation because of a poorly predicted trend.

**Even while
AI and ML
have
amazing
potential,
they are far
from
foolproof.**



Navigating the Double Edged Sword

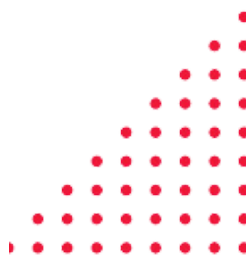
We should take a moment to consider whether we are depending too much on these technologies in our quest for advancement. Shouldn't we take precautions against relying too much on potentially flawed systems? It's important that we understand that technology is a tool, not a substitute for human judgment

Navigating the Balance: Risk Strategies for all levels Navigating the double-edged nature of AI and ML means balancing potential with caution. Here is how you can solve the problem at different levels:

For New Professionals: Begin with curiosity paired with caution. Take time to understand the systems your organization relies on, question the sources and inputs, and don't settle for just what's convenient. If you're unsure, reach out to your team, remembering that in risk management, asking the right questions can be as valuable as finding the answers.

For Seasoned Experts: Set the standard by modeling a thorough approach to AI oversight. Stress the importance of transparency by considering not only the results the AI provides but also the reasoning behind them. Guide your team to focus on data security, model clarity and ethical practices; recognizing that a single data breach or bias issue could quickly erode years of trust.

It's possible
that an
algorithm is
collecting
and
modifying
data in the
background
to take
advantage of
our trust.



Navigating the Double Edged Sword

Ethics and Responsibility: A Moral Crossroad

As we enthusiastically adopt AI and ML, we are also approaching a moral juncture. Although face recognition technology makes it simple to unlock our phones, it also records and archives our identities, making us data points that are monitored by an extensive network of surveillance cameras.

The key question is, are we prepared to demand transparency and accountability from these systems? Are we ready to advocate for ethical use, knowing that our voices will determine how AI shapes our future? As users, we depend on the creators of these tools, but we also have the power to drive change by supporting platforms and services that respect our values.

Conclusion: Embracing AI with Vigilance and Vision

AI and ML are not going to be sunshine and rainbows nor are they going to be all doom and gloom, they are going to be a mixture and that mixture is going to depend on how well and effectively these tools are leveraged. Massively, every risk professional will be able to build a better tomorrow, where AI and ML are pivotal in transforming the world, yet with respect to Control, Privacy and Ethics.

So, enjoy the 'Digital Era' trip, making room both for creativity and steadfastness!

The author is Vice President with a Fortune 500 Company and currently pursuing her Doctorate in Artificial Intelligence. The views expressed are her own.

The key question is, Are we ready to advocate for ethical use, knowing that our voices will determine how AI shapes our future?

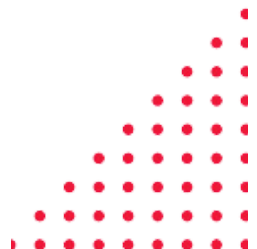
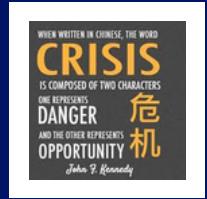


Veena Jadhav



Risk Management Careers

- Careers in Risk Management
- Key Skills for Existing Risk Executives
- Professionals transitioning to Risk Management
- Future Ready CROs



Careers in Risk Management

Growing Demand for Risk Professionals:

1. Increased demand from traditional sectors like Financial Services, Banks, Insurance companies, Healthcare and Energy, Big 4s and Consulting firms.

2. Growing demand from emerging sectors like startups, including Fintech firms, PE Funds, Family owned businesses and Medium and Small Enterprises.

3. Variety of Roles on Offer

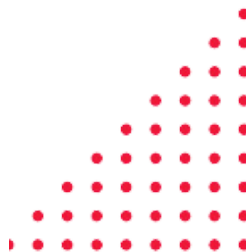
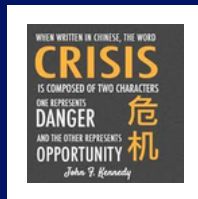
a) Generalist like ERM Managers or specialized in particular domain- e.g digital risk, Cyber Security experts,

b) Working with Business to manage risks (First Line of defence) or in Advisory /Oversight roles (Second line of defence).

Skills Required:

1. Functional and Domain Knowledge
2. Analytical and Problem Solving skills
3. Understanding of the Business
4. Communication and Interpersonal skills
5. Ability to challenge respectfully
6. Negotiation and stakeholder management

Majority of the organisations, while hiring candidates for various risk roles, prefer candidates with risk certification in addition to them possessing relevant technical and leadership skills



Careers in Risk Management

Responsibilities and Career Progression:

Risk Analyst/Officer (3.00 L- 10.00 L P.A):

- Execute on risk assessment programs
- Conduct Testing and assurance review
- Track KRI's
- Provide Analytics

Risk Manager/AVP (15.00 L - 30.00 L P.A):

- *Execute on the Risk Strategy and Roadmap*
- *Review the results from various risk assessments*
- *Track Significant events and KRI*

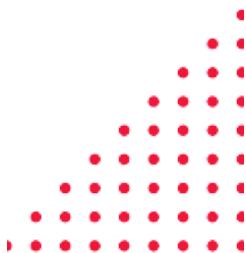
Risk VP/Director (40.00 L- 60.00 L P.A):

- Lead the execution of Risk Strategy in partnership with Business heads
- Review significant risks facing the business with the Business heads
- Highlight significant issues and KRI breaches to CRO and Risk Committee

Risk Head/Chief Risk Officer (75.00 L- 100.00L P.A):

- Develop and present Risk strategy to the Board
- Review regulatory findings with Risk Committee
- Review significant and material risk events at company level with CEO

There are varieties of options available in today's world to make career in risk management with well defined career progression.



Careers in Risk Management

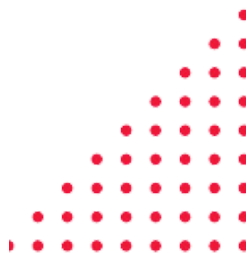
In summary:

We are living in unprecedented times (VUCA world), the business environment and consequently the risk landscape has evolved considerably over last few years and these changes and corresponding risks have been further accelerated post the 2019 Pandemic.

Many businesses after responding to the events triggered by COVID 19, are now beginning to reshape the way they do things, right from rewriting the customer playbook, reassessing their supply chain models, adopting new technology and thinking about future workplace.

Risk Managers have a big role to play in working with Board, Senior Management and Business Leaders in not only helping them manage through these turbulent times but also to ensure that they are proactively partnering to use this crisis as an opportunity to create a more operationally resilient organisation.

**Risk
Managers
have a big
role to play
in working
with Board,
Senior
Management
and
Business
Leaders in
helping them
manage
through
these
turbulent
times.**



Careers in Risk Management

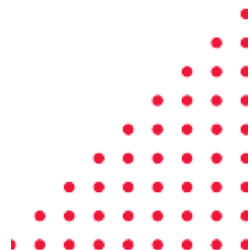
Enterprise Risk Management (ERM) is used by organizations to identify, monitor evaluate and manage risks within their businesses.

While ERM has existed for may years, especially in Financial Services and Banking Industry, it has gained greater prominence through some of the big events in last 15-20 years including Enron and WorldCom scandals and other corporate failures, financial crisis of 2008 and COVID pandemic of 2021 to name a few.

ERM is being adopted by organisations to not only to comply with regulatory guidelines but also to manage their risks more effectively and utilize their capital more efficiently. It is also being seen by the organisations as a tool to drive competitive advantage.

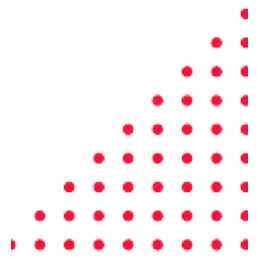
ERM covers entire gamut of risks that can be considered under its umbrella, from Operational risk, Business continuity and resiliency, Digital risk, Personnel risk, physical and logical security and internal and external fraud.

ERM covers entire gamut of risks that can be considered under its umbrella, from Operational risk, Business continuity and resiliency, Digital risk, Personnel risk, and internal and external fraud.



Risk Management Careers

- Careers in Enterprise Risk Management (ERM)
- Key Skills for Existing Risk Executives
- Professionals transitioning to Risk Management
- Future Ready CROs



Key Skills for Existing Risk Executives

"I have the requisite skills and experience but I am not even getting shortlisted for the risk executive job that I had applied for "

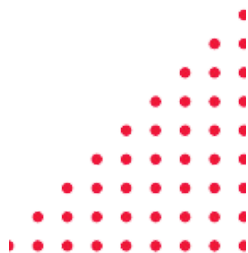
"I have gone above and beyond and delivered on all my goals and objectives but I am not getting enough appreciation and credit for what I am doing"

I have heard these and other similar comments from Risk Executives who reach out to me for career coaching. My advice to them is very simple starting with the fact that business environment is changing rapidly leading to ever evolving and complex risk landscape which is making their job much more difficult and secondly the expectations from their leaders, board, management and regulators have undergone a big change.

It is one thing to have the right technical knowledge of enterprise risk management concepts and framework but risk executives should be able to demonstrate the right leadership skills to showcase their contributions to meeting organization's objectives, like their ability to proactively engage with business partners, ability to develop and create risk programs from ground up that are practical and pragmatic and so on.

I have compiled these top key skills that every risk executive should be able to demonstrate to be successful.

Risk executives should be able to demonstrate the right leadership skills to showcase their contributions to meeting organization's objectives, like their ability to proactively engage with business partners.



Key Skills for Existing Risk Executives

Effective Implementation of ERM Concepts

While having conceptual knowledge of ERM is essential for risk executives to fulfill their responsibilities, it is equally crucial for them to showcase practical examples of how they utilized risk concepts and frameworks to implement risk programs that are pragmatic, practical, effective, efficient and address the unique needs of the organization.

Complexity and Breadth of their Work

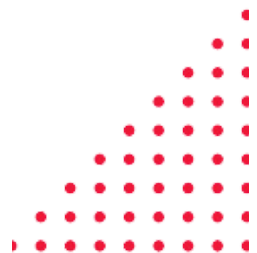
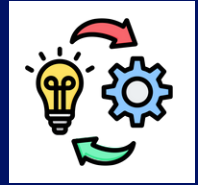
Risk executives should be able to demonstrate the breadth and complexity of their roles by highlighting the variety of diverse risks programs they manage, the number of key stakeholders they partner with and diverse functions they support. Risk Executives can also talk about strategic decision-making involved and the impact on organizational success through the programs led by them.

Engagement with Business

Risk executives should be able to demonstrate how they proactively engage with their business partners to not only address their control issues as and when they happen but also assist them in achieving their business objective (for e.g, support during new product launches, signing up a new client, on-boarding new vendor and actively partnering in transformation initiatives).

Elevating Risk Excellence Culture

Culture play a very critical role as far as the success of any organization is concerned. Risk executives should be able to demonstrate how they elevated the culture of risk excellence within an organization at all levels. This could be done by demonstrating increase in self identified issues, reduction in mandatory training defaults etc.



Key Skills for Existing Risk Executives

Drawing Insights from Data

Risk executives should not only be satisfied with providing data on how and why the errors happened. They should be able to demonstrate how they used the insights from data to work collaboratively with business in managing the risk proactively and prevent issues from happening in future, thereby enhancing the organization's ability to achieve its objectives.



Developing External Perspective

Risk executives should be able to demonstrate that they are connected with outside world by continuously monitoring the external events to assess how these can potentially impact their organization. They should also be able to demonstrate their understanding of emerging risks, and tools technologies that are available to mitigate the emerging and current risks.



Providing Effective Challenge

Risk executives (especially second line) should be able to demonstrate that they are independent of business through effective challenge which ultimately protects the interest of business and assist them in achieving their business objectives.



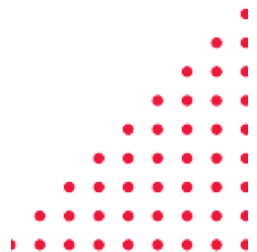
Building and Nurturing Talent

As the new risks emerge, risk executives should be able to demonstrate not only how they are upskilling themselves and keeping pace with the changes in the risk landscape, but also how they are ensuring their teams are well equipped to handle the new and complex scenarios in a proactive manner.



Risk Management Careers

- Careers in Enterprise Risk Management (ERM)
- Key Skills for Existing Risk Executives
- Professionals transitioning to Risk Management
- Future Ready CROs



Professionals Transitioning to Risk Management

"I want to get out of my current operations role and switch to risk management but it has been more than 1 year and I am still not able to find a relevant opening"

"I was hoping that once I complete my certification in risk, I will get opportunity to work in risk department of big corporate of one of the big 4 accounting firms but I am not making any headway"

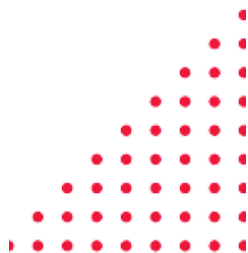
These and similar questions is what I get from people, who are either recent graduates or existing professionals trying to switch their career in risk management, when they come to me for #mentoring advice and coaching.

Whether you are a recent graduate or looking to make a career shift in risk management, there are few steps that you need to undertake like acquiring a formal risk qualification, networking, interning or volunteering for risk projects creating your personal brand and finding the right mentor or coach, these are the "must haves" for a smooth transition into risk related roles.

Read on in more details how you can increase your chances of switching to career in risk management and what all it takes to make a smooth transition.

Remember, a career switch in risk management requires right planning, consistent efforts, perseverance and guidance from senior pros. But with determinations and right approach you can successfully pivot into a rewarding.

Career switch in risk management requires right planning, consistent efforts, perseverance and guidance from senior pros. But with determinations and right approach you can successfully pivot into a rewarding career.



Professionals Transitioning to Risk Management

Self Assessment and Research

Anyone wanting to switch to a career in risk management need to assess if risk management is the right career for them in long term, along with skills required, their existing capabilities and any skill gaps that they need to address, both in short and long term. Reach out to someone who is already in this space to understand what does the job entails, skills that are required and how a day in life of risk manager looks like before taking the plunge.

Invest in Formal Certification

Risk Management is becoming increasingly specialized discipline and hiring managers are looking for people who have undertaken formal education in risk management and are well versed with various risk frameworks and standards. People wishing to make their career in risk management should seriously consider investing in a good risk management program that offers comprehensive curriculum, globally accepted certification, strong alumni and placement support.

Start with a Small Side Project

While getting a risk certification will open doors for you, a small side project related to risk could be your launch pad to get into risk management full time. It will provide you the practical experience and demonstrate your commitment and seriousness to potential employers. You could do this by volunteering for a risk or assurance review in your department or act as an SME for audit or regulatory exam in your current organization.



Professionals Transitioning to Risk Management

Try the Lateral Move

While looking to switch careers, taking a lateral move either within the current organization or outside could be a really potent move. Remember, your probability of landing a job (when you are switching careers) with a lateral move is much higher as compared to someone betting on you for a next level with a career change.



Attend Seminars, Industry Events

With rapidly changing business environment and constantly evolving risk landscape, It will be worthwhile for the people wanting to make their career in risk management to invest their time in attending industry events and seminars and try to keep pace with all the changes and advancements that are happening in this field. Added Bonus: you get to network with people who can help you in your career.



Focus on Networking

Networking is absolutely critical if you are trying to switch jobs or looking for a career change. It opens doors to industry insights, mentorship and potential job leads Invest your time in building deep and diverse networks both with your current connections and with broader set of people who can assist and guide you in your journey.



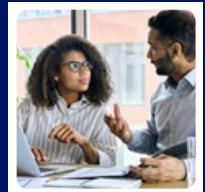
Professionals Transitioning to Risk Management

Work in a Cross Functional Project

Volunteering for risk focused cross functional projects in your current organization further solidifies your seriousness in pursuing the risk career and provides you with an opportunity to test your concepts and knowledge in practical scenarios. Moreover, it also provides you with an opportunity to create strong and deep networks that could help you in your future job search.

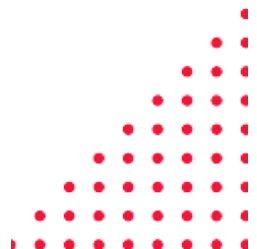
Get a Mentor or Coach

Getting a coach or mentor is the best investment you can make to help you during this journey. They are your guiding light and can provide you with tailored advice, share their experience and wisdom, help you steer through your journey, connect you to the right people, help you navigate and open doors for you with other people in their network.



Risk Management Careers

- Careers in Enterprise Risk Management (ERM)
- Key Skills for Existing Risk Executives
- Professionals transitioning to Risk Management
- Future Ready CROs



Future Ready CRO

Are you "Future Ready CRO?"

Last week, while talking to few friends who are Chief Risk Officers (CROs) and Head of Enterprise Risk in reputed organizations, I heard almost all of them sounding overwhelmed with the velocity of changes happening around them, manifestation of variety of risks, them being in perennially fire fighting mode and lack of support from Business and Senior leaders.

What I have realized from these discussion is that the role of CRO has been thrust into limelight in last few months due to high profile failures of SVB, Credit Suisse etc and the expectations from CROs have changed drastically in last few years. While some of the CROs have made this transition seamlessly, many of them are struggling with increased expectations from Board, Audit Committee, Regulators and Stakeholders

CROs, according to me need to engage and PARTNER more deeply with their stakeholder to manage this volatile business environment and risks effectively and efficiently. In addition to possessing technical expertise to manage existing and emerging risks, they also need to demonstrate resiliency, adaptiveness and be able to navigate the complex organization systems and hierarchy.

Read on to see what PARTNER means and how it can help you to become "future ready CRO"

CROs, a need to engage and PARTNER more deeply with their stakeholder to manage this volatile business environment and risks effectively and efficiently.



Future Ready CRO

CROs, need to engage and PARTNER more deeply with their stakeholder to manage this volatile business environment and risks effectively and efficiently. In addition to possessing technical expertise to manage existing and emerging risks, they also need to demonstrate resiliency, adaptiveness and be able to navigate the complex organization systems and hierarchy.

P

CROs must adopt a proactive stance in managing risks by constantly scanning the horizon for emerging risks and opportunities, identifying vulnerabilities and implementing preventive measures. CROs can minimize surprises and help business in maintaining competitive edge with their proactive approach.

A

CROs who are adaptable and take flexible approach to risk management can anticipate changes, adjust risk strategies, take proactive measures and are able to use the organization's resources more effectively and efficiently.

R

CROs need to be resilient in this era of volatility . Resilience allows them to adapt swiftly to unforeseen challenges, bounce back from setbacks and instill confidence in their stakeholders. Their ability to navigate uncertainties and seize opportunities ensures long term success and stability of the organization.

PARTNER

Proactive
Adaptable
Resilient
Tech Savy
Navigator
Engaged
Realistic



Future Ready CRO

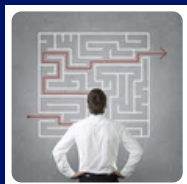
T

CROs must be tech-savvy and be able to harness the power of technology to effectively manage risks in today's digital landscape. CROs need to understand emerging technologies, data analytics, cybersecurity and digital threats to proactively safeguard the organizations from these risks.



N

CROs must excel at navigating the organizational maze to effectively manage risks. . By mastering the organizational landscape, CROs can ensure that risk management strategies align with business objectives and gain support from relevant stakeholders for effective risk management initiatives.



E

By proactively engaging with relevant stakeholders, CROs gain valuable insights, ensure risk awareness, enhance risk culture, and foster collaborative decision making. Engaging with diverse perspective enables better risk assessment, mitigation and ultimately strengthens risk excellence culture in an organization.



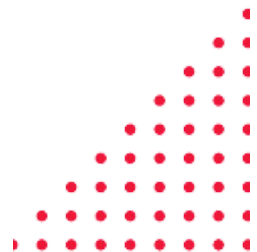
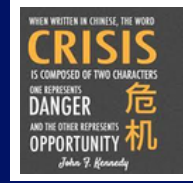
R

CROs must provide a realistic picture of risks to all stakeholders to help them take informed decisions. By accurately assessing and communicating risks, CROs ensure transparency, build trust, and enable effective risk mitigation. Realistic insight empowers stakeholders to make informed choices, enhancing the organization's ability to achieve its objectives



Additional Resources

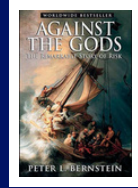
- Risk Management Books
- Scams and Frauds
- Risk Management Movies



Books on Risk Management

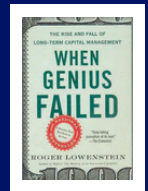
1. AGAINST THE GODS - - Peter L Bernstein

In this book, Peter L Bernstein, provides valuable insights into the cultural, social, and political factors that have shaped our understanding of risks, as well as the ways in which advances in science and technology have transformed this field.



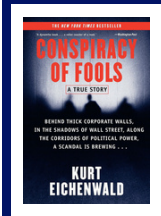
2. WHEN GENIUS FAILED - - Roger Lowenstein

True story of how LTCM's founders, who were renowned experts, including Nobel Prize winners, used complex financial models to take risky bets in global financial markets and suffered catastrophic losses.



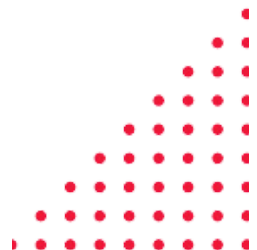
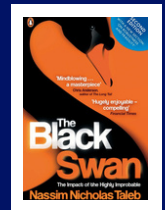
3. CONSPIRACY OF FOOLS - Kurt Eichenwald

Award-winning New York Times reporter, Kurt Eichenwald provides a detailed account of the corporate culture at Enron, as well as the actions of key executives and other stakeholders that ultimately led to the company's collapse.



4. THE BLACK SWAN -Nassim Nicholas Taleb

"The Black Swan" offers insightful perspective on risk and uncertainty, and provides variety of examples about the unpredictability of events and the dangers of relying too heavily on statistical models and assumptions.



Books on Risk Management

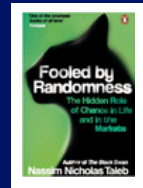
5. TOO BIG TO FAIL -Andrew Ross Sorkin

"Too Big to Fail" discusses the origins of the 2008 financial crisis, including the housing bubble, subprime mortgage market, and the use of complex financial instruments such as Credit Default Swaps



6. FOOLED BY RANDOMNESS -Nassim Nicholas Taleb

Nassim Nicholas Taleb, explores the role of luck and randomness in our lives, particularly in the context of financial markets and investment decisions and the dangers of over relying on past performance and historical data to make investment decisions.



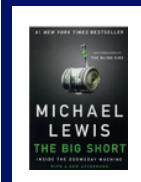
7. THE BILLIONAIRE'S APPRENTICE -Anita Raghavan

Anita Raghavan- the award-winning journalist tells the story of collapse of Galleon Hedge fund and the rise and fall of Rajat Gupta, a former CEO of McKinsey & Company and a board member of several major corporations.



8. THE BIG SHORT -Michael Lewis

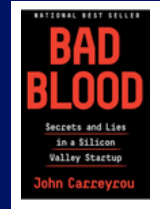
"The Big Short" by Michael Lewis tells the story of a group of investors who saw the 2008 financial crisis coming and bet against the housing market.



Books on Risk Management

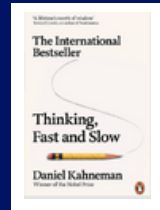
9. BAD BLOOD- -John Carreyrou

"Bad Blood" by John Carreyrou describes the rise and fall of Theranos, a Silicon Valley startup, and provides a detailed account of the company's fraudulent practices, as well as the actions of its founder and key executives.



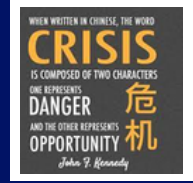
10. THINKING FAST AND SLOW -Daniel Kahneman

Daniel Kahneman's book provides valuable insights into the risks and challenges of decision making in a variety of contexts.



Additional Resources

- Risk Management Books
- [Scams and Frauds](#)
- Risk Management Movies



Biggest Scams and Frauds

1. Barings- Nick Leeson

Nick Leeson's speculative trading and concealment of losses in a secret account caused the collapse of Barings Bank in 1995, resulting in losses of over \$2 B. The scandal exposed flaws in risk management and led to regulatory reforms. Leeson was sentenced to six and a half years in prison.



2. The London Whale

The JP Morgan scandal involved a trader in its London office, who became known as the "London Whale" and caused whopping \$6 B in trading losses on a specialized derivatives portfolio and almost \$1 B in penalties. This scandal became the catalyst for regulators to finalize new rules banning publicly insured banks from speculative trading.



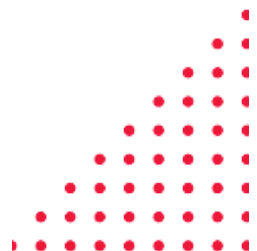
3. The Enron Scandal

Enron executives committed accounting fraud and manipulated energy prices, causing Enron's collapse in 2001, leading to losses for investors and employees. The scandal exposed flaws in corporate governance and accounting practices, resulting in the passage of the Sarbanes-Oxley Act. Enron's CEO and chairman were convicted and sentenced for securities fraud and conspiracy.



4. The Satyam Scam

Satyam founder Ramalinga Raju admitted to falsifying accounts and inflating profits in 2009, leading to loss of investor confidence, government takeover, and criminal charges for Raju and his associates. The case highlighted the need for improved corporate governance and regulation in India.



Biggest Scams and Frauds

5. The IL&FS Scam

IL&FS engaged in fraudulent accounting practices, mismanagement of funds, and over-borrowing, leading to a liquidity crisis and defaults on debt obligations in 2018. The scandal exposed flaws in the governance of NBFCs in India, and the government took control of the company.



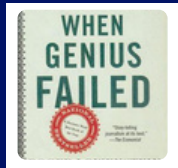
6. The Harshad Mehta Scam

Harshad Mehta manipulated stock prices using funds fraudulently obtained from banks in 1992, leading to a massive stock market crash and exposing flaws in the regulation of the Indian stock market and banking system. Mehta was arrested and charged with multiple offenses. The case led to the establishment of SEBI to regulate the securities market in India



7. LTCM Collapse

LTCM was a hedge fund that collapsed in 1998 due to complex leveraged trading, causing a liquidity crisis. The U.S. Federal Reserve intervened to prevent a broader financial crisis. The case raised concerns about systemic risks, regulation, and interconnectivity of global financial markets.



8. The Subprime Mortgage Crisis

The subprime mortgage crisis occurred in 2008 due to high-risk mortgage loans defaulting, causing a decline in housing prices and a wave of foreclosures. It led to significant losses for banks and financial institutions, a global economic recession, and increased regulatory oversight.



Biggest Scams and Frauds

9.FTX Collapse

In Nov 2022, FTX crypto exchange collapsed from a liquidity crisis caused by Alameda Research's token ownership. Fraud investigations, bankruptcy, CEO resignation, and significant industry repercussions followed, with Bankman-Fried's net worth taking a hit.



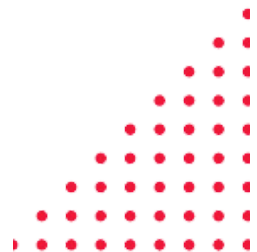
10.Wells Fargo Fraud

Wells Fargo, a US bank, was found to have created millions of unauthorized customer accounts between 2011 and 2016. The scandal resulted in a \$185 million settlement with regulators and the resignation of CEO John Stumpf.



11.Theranos

Theranos was a health technology company that falsely claimed to have developed fast and accurate blood tests using small amounts of blood. The fraudulent claims led to legal and commercial challenges, with the company and its founders being charged with fraud, Elizabeth Holmes being found guilty, and the dissolution of the company in 2018.



Biggest Scams and Frauds

12. Volkswagen Emissions Scandal

Volkswagen, a German car company, was involved in a scandal where they installed software in their diesel cars to cheat emissions tests. This was discovered in 2015 and resulted in fines, lawsuits, and a drop in the company's stock price.



13. Lehman Brothers

Lehman Brothers' bankruptcy in 2008 triggered a global financial crisis, causing social and economic consequences. Regulatory reforms were implemented to increase transparency and accountability in the financial sector, highlighting the need for more responsible practices.



14. The WorldCom Scandal

WorldCom's executives manipulated accounting records, causing a \$11B scandal, leading to bankruptcy, convictions of CEO and CFO, and increased need for regulation and governance oversight.



15. Jerome Kerviel Socgen

Société Générale trader Jérôme Kerviel caused a €4.9B loss through unauthorized trades in 2008. Arrested and convicted in 2010 for breach of trust, forgery, and computer misuse, his case spotlighted risk management in banking. Kerviel claimed his superiors were aware, but Société Générale disputed this.



Biggest Scams and Frauds

16. Bernie Madoff Ponzi Scheme

Bernie Madoff ran a Ponzi scheme, defrauding thousands of investors out of billions of dollars. The scheme collapsed during the 2008 financial crisis, and he was sentenced to 150 years in prison. The scandal exposed flaws in financial market regulation and led to the creation of SIPC to protect investors against fraud.



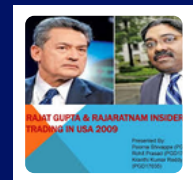
17. Citi Revlon

Citigroup mistakenly sent \$900 million to Revlon's lenders in 2020, who refused to return the funds. Citigroup lost the lawsuit to recover the funds, highlighting risks in complex financial transactions and the importance of risk management and communication.



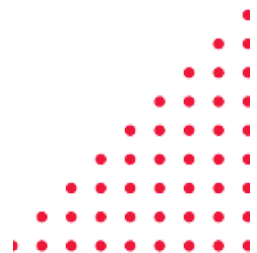
18. Rajat Gupta Insider Trading

McKinsey's ex-consultant Rajat Gupta was imprisoned for insider trading in 2012, having shared secret details on Goldman Sachs and Procter & Gamble with hedge fund founder Raj Rajaratnam. Gupta sat on both companies' boards. He was fined \$5M, jailed for two years, and freed in 2016, underscoring the significance of ethical business practices.



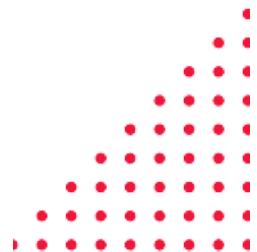
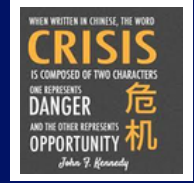
19. The 1Malaysia Development Berhad (1MDB) Scandal

The 1MDB scandal involved the theft of billions of dollars from a Malaysian government fund through corruption and money laundering. Jho Low allegedly masterminded the scheme, and former Malaysian Prime Minister Najib Razak and Goldman Sachs were implicated. It triggered criminal investigations and a \$2.9 billion settlement for Goldman Sachs.



Additional Resources

- Risk Management Books
- Scams and Frauds
- Risk Management Movies



Movies on Risk Management

1.WALL STREET

"Wall Street" is a classic film that explores ambition, greed, and ethics in finance. . The movie offers a critical look at the stock market, insider trading and the consequences of unchecked corporate power.



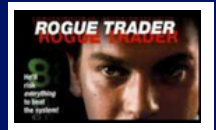
2.MARGIN CALL

"Margin Call" is a 2011 drama film about a fictional investment bank's discovery of catastrophic losses from risky mortgage-backed securities. The movie offers a critical perspective on the financial industry and highlights the human costs of corporate greed and recklessness.



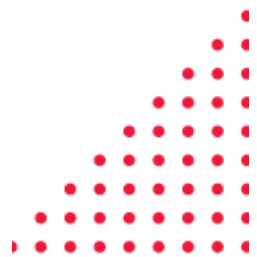
3.ROUGE TRADER

"Rogue Trader" is a 1999 biographical drama about Nick Leeson, a trader who caused the collapse of Barings Bank in 1995. The movie depicts the consequences of unethical behavior and unchecked risk-taking.



4.THE BIG SHORT

"The Big Short" is a 2015 biographical drama about a group of investors who predicted the 2008 financial crisis. The movie critiques the financial industry and highlights the greed and corruption that led to the crisis, while offering a compelling portrayal of those who saw the impending disaster and profited from it.



Movies on Risk Management

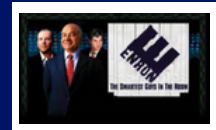
5. BAD BOY BILLIONAIRES INDIA

"Bad Boy Billionaires: India" is a 2020 documentary series exploring the lives and controversies of infamous Indian business magnates, shedding light on their lavish lifestyles, corrupt practices, and legal troubles, and examining their impact on Indian society and the economy.



6. ENRON-THE SMARTEST GUYS IN THE ROOM

"Enron: The Smartest Guys in the Room" is a 2005 documentary exposing the fraudulent accounting practices and complicity of executives and auditors in the rise and fall of Enron Corporation, one of the largest corporate scandals in American history, and its devastating impact on the economy and stakeholders.



7. TOO BIG TO FAIL

"Too Big to Fail" is a 2011 HBO film that offers an inside look at the decision-making process and controversial bailouts of major financial institutions during the 2008 financial crisis, highlighting the complex relationships between bankers, politicians, and regulators.



8. THE WOLF OF WALL STREET

"The Wolf of Wall Street" is a 2013 film based on the true story of Jordan Belfort, a fraudulent stockbroker whose wealth and excesses led to his downfall. Directed by Martin Scorsese and starring Leonardo DiCaprio, the film offers a darkly comedic portrayal of the greed and corruption of Wall Street in the 1990s.



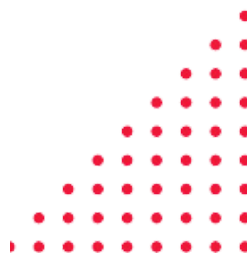
9. INSIDE JOB

"Inside Job" is a 2010 documentary exposing systemic corruption and conflicts of interest in the financial industry that contributed to the 2008 global financial crisis, and calls for urgent reform and accountability to prevent future crises.



10. SCAM 1992 (SONY LIV)

"Scam 1992" is a Hindi-language web series based on the true story of Indian stockbroker Harshad Mehta and his involvement in a series of financial scams in the late 1980s and early 1990s. The show depicts Mehta's rise to power, downfall, and the legal and political consequences of his actions.



Acknowledgement

Bringing this second edition of this eBook to life has been a collaborative endeavor, and I am deeply grateful to the individuals who dedicated their time, expertise, and creativity to make it a reality.

First and foremost, I would like to express my sincere gratitude to Syed whose insightful suggestions have significantly enhanced the clarity and quality of the material.

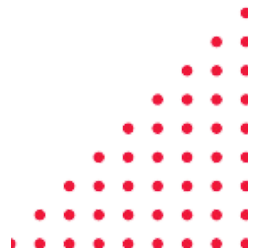
I would also like to thank Major General Neeraj Bali, SM (retd), Dr. Aneish Kumar, Nishtha Khurana and Veena Jadhav who have contributed immensely to the credibility of this eBook by sharing their perspective and articles.

This eBook would not have been possible without the love and support of our linkedin family members. Your contributions, suggestion and comments on my linkedin posts have made it more than just a collection of words; and has helped me to hopefully create a meaningful resource that I hope will benefit and inspire readers of this subject.

With heartfelt thanks,
Jitu Arora
Founder and CEO Beyond RisX



Syed Jafri-ICA



About Beyond RisX

Beyond RisX envisions a world where risk is understood, managed, and transformed into opportunities and competitive advantage.

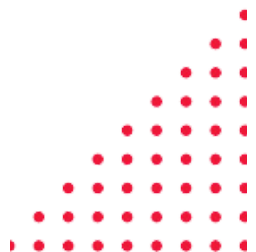
Through engaging courses and workshops in educational institutions, enlightening seminars and customized workshops for corporates, insightful consulting services, and personalized career coaching, we empower individuals and organizations to navigate the complex landscape of risk with confidence and foresight.

By fostering a culture of risk awareness and competence, Beyond RisX strives to catalyze innovation, resilience, sustainable growth and competitive advantage for both individuals and organizations.

Beyond RisX is an effort of likeminded Senior Risk professionals with extensive industry experience to come together and address the lack of awareness about risk management as a discipline and a career choice, embed the risk mindset in individuals, elevate the risk excellence culture in organizations and equip them to use risk as a competitive advantage.

Our founders, advisory board members, mentors, coaches and speakers are all eminent and senior industry professionals, from prestigious institutes like Cornell, UCLA, IITs and IIMs who have worked with organizations like JP Morgan, American Express, Credit Suisse, Wells Fargo, Standards and Poor's, Sunlife, Standard Chartered, State Street, Deloitte and Infosys to name a few and are bound by a common vision to build next generation of successful risk leaders by sharing their learning with them and coaching and mentoring them to be successful.

**Beyond RisX
is an effort to
embed the
risk mindset
in individuals,
elevate the
risk
excellence
culture in
organizations
and equip
them to use
risk as a
competitive
advantage.**



Connect With Us



info@beyondrisx.com



+91-9717272279



[BeyondRiskx](https://beyondrisx.com)



<https://beyondrisx.com>

