Mayank Sharma

Document2

Major Research Project

Document Details

Submission ID
trn:oid:::27535:147005071

Submission Date
Jul 31, 2026, 6:29 PM GMT+5:30

Download Date
Jul 31, 2026, 6:32 PM GMT+5:30

File Name
Document2.docx

File Size
408.3 KB

39 Pages

8,813 Words

53,909 Characters

8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Small Matches (less than 10 words)

Match Groups

20 Not Cited or Quoted 8%
Matches with neither in-text citation nor quotation marks

1 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

8% Internet sources
4% Publications
7% Submitted works (Student Papers)

Match Groups

- **20** Not Cited or Quoted 8%
  Matches with neither in-text citation nor quotation marks
- **1** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

8% Internet sources
4% Publications
7% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
preteshbiswas.com		2%
2	Internet	
www.coursehero.com		<1%
3	Student papers	
Delhi Technological University on 2026-05-28		<1%
4	Internet	
www.lakegrace.wa.gov.au		<1%
5	Internet	
www.merriam-webster.com		<1%
6	Student papers	
Delhi Technological University on 2024-05-23		<1%
7	Student papers	
Delhi Technological University on 2026-05-29		<1%
8	Student papers	
Delhi Technological University on 2026-06-12		<1%
9	Student papers	
Universiteit van Amsterdam on 2019-08-13		<1%
10	Student papers	
Australia Financial Markets Pty Ltd on 2018-02-26		<1%

11 Student papers

Australia Financial Markets Pty Ltd on 2020-11-12 <1%

12 Student papers

International University Schloss Reichardshausen on 2013-02-13 <1%

13 Student papers

BRAC University on 2025-04-26 <1%

14 Internet

etraverse.com <1%

15 Student papers

BB9.1 PROD on 2026-07-31 <1%

16 Internet

www.pharmavalidation.in <1%

17 Internet

p3m.ppns.ac.id <1%

ENTERPRISE RISK MANAGEMENT

14

Thesis Submitted
in Partial Fulfilment of the Requirements for the
Degree of Masters of
Business Administration
In
Data Science and Analytics

Archit Vats
14/UEMBA/01

8

UNDER THE SUPERVISION OF

Dr Anurag Chaturvedi

Assistant Professor

DELHI TECHNOLOGICAL UNIVERSITY



DEPARTMENT OF MANAGEMENT AND ENTREPRENEURSHIP
DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-110042, India

AUGUST 2026

CANDIDATE'S DECLARATION

I, ARCHIT VATS, hereby certify that the work which is being presented in the thesis entitled ENTERPRISE RISK MANAGEMENT in partial fulfilment of the requirements for the award of the Degree of Master of Business Administration, submitted in the Department of MANAGEMENT AND ENTREPRENEURSHIP, Delhi Technological University, is an authentic record of my own work carried out during the period from 08-06-2026 to 01-09-2026 under the supervision of Dr Anurag Chaturvedi.

The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other institute.

Candidate's Signature

Archit Vats (24/UEMBA/01)

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis, and the statement made by the candidate is correct to the best of our knowledge.

Signature of Supervisor(s)

Signature of External Examiner

CERTIFICATE BY SUPERVISOR

Certified that Archit Vats (24/UEMBA/01) has carried out their search work presented in this thesis for the award of Master of Business Administration from the Department of Business Administration, Delhi Technological University, Delhi, under my supervision. The thesis embodies results of original work, and studies are carried out by the student himself, and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other university/institution.

Signature of Mentor

Dr Anurag Chaturvedi

Assistant Professor

ACKNOWLEDGEMENT

I express sincere thanks to our faculty mentor for giving us valuable time and inspiring cooperation towards the project, which could not have been a success without his guidance. Lastly, I would like to thank every person who has been responsive and welcoming throughout this project for providing me with all the necessary help to make this project a success.

Archit Vats (24/UEMBA/01)

13

Table of Contents

CANDIDATE'S DECLARATION 1
CERTIFICATE BY SUPERVISOR 2
ACKNOWLEDGEMENT 3
List of Figures 6
List of symbols and Abbreviation 6
List of Tables 6
EXECUTIVE SUMMARY 7
Chapter I: INTRODUCTION AND FOUNDATIONAL PARADIGMS 8
What is an enterprise? 8
What is Enterprise Risk Management: 8
Enterprise risk according to governing authorities 8
Big 4 Definitions and differences 10
Chapter II: Case Study 12
EXECUTIVE SUMMARY & COMPANY PROFILE 13
Case Study: Zippyy.ai – Enterprise Risk Management Through Agentic AI 13
Operational Architecture 13
Software as a service model: 13
Delivery partner: 14
Competitive Differentiators 14
Chapter III: Literature Review 15
Defining the Risk Universe 15
Risk Identification and Risk inventory management 15
Core Methods of Risk Identification 15
Steps to Establish a Comprehensive Risk Inventory 16
Core Mitigation Techniques 17
Formulas to Calculate WHEN to Mitigate Risk 20

16

Failure Mode and Effects Analysis (FMEA) – Risk Priority Number (RPN) 20
Formulas to Calculate HOW MUCH to Invest in Mitigation 20
Advanced Quantitative Modelling Alternatives 21
COSO Framework 22
The Paradigm Shift: 2004 vs. 2017 22

The Five Core Components and 20 Guiding Principles 23
Principles of COSO model 23
ISO Framework 27
Principles (The Philosophy) 27
Framework (The Organizational Infrastructure) 28
Process (The Operational Execution) 29
Importance of Enterprise Risk Management 30
Chapter IV: Analysis 32
The Top Five Emerging Risks Landscape (2Q26) 32
The rapid rise of this threat is fueled by three main drivers 32
Potential Consequences for Enterprises 33
Macro Risk Context: Gartner Research on Agentic AI 33
Gartner Bow-Tie Root Cause & Impact Mapping for Agentic AI 33
Zippy.ai Dilemma: Agentic Autonomy vs. Human-in-the-Loop 34
The Human-in-the-Loop (HITL) Threshold Control 34
The Risk Event Scenario 34
Integrated ERM Framework Coupling (COSO + ISO 31000 + NAVI) 35
Chapter V: Conclusion 38

List of Tables

Table No.	Title
Table 1.1	Comparison of Enterprise Risk management within big 4
Table 3.1	Mitigation methods description and trade-offs

List of Figures

Figure No.	Title
Figure 3.1	
Figure 3.2	
Figure 4.1	
Figure 4.2	Gartner Bow tie Root cause and impact mapping

List of Abbreviations and Symbols

Symbol	Value
ERM	Enterprise Risk Management
ISO	International organization of Standardization
COSO	Committee of Sponsoring Organizations of the Treadway Commission
PWC	PricewaterhouseCoopers
EY	Ernst & Young
DTC	Direct-to-Consumer
FMEA	Failure Mode and Effects Analysis
RPN	Risk Priority Number

EXECUTIVE SUMMARY

Enterprises have an innate risk that they undertake in any market or set up these risks come from changes in technology, legal environment, compliance or environmental scenarios. These risks can have high financial impact, reputation loss, oh complete breakdown of an enterprise but they also allow for value creation and opportunities to gain a competitive edge. In today's landscape of uncertainties and dynamic changes occurring across the landscape enterprises must manage the impact from these uncertainties and structural shifts. Traditional methods to find these risks and its impact in financial, reputational, legal framework can no longer be used.

This report covers methods to identify, calculate the impact of the consequences, mitigate and monitor for future analysis of risks.

We utilise the 2 primary frameworks off COSO and ISO 31,000: 2018 to find the best approach while working with the risk.

This report also covers a practical application of the literature review by utilising a case study of zippy.AI to utilise the methodology found in the literature.

Chapter I: INTRODUCTION AND FOUNDATIONAL PARADIGMS

What is an enterprise?

According to Merriam Webster

enterprise

noun

en·ter·prise ˈen-tər-ˌprīz

1. A project or undertaking that is especially difficult, complicated, or risky
2.
    a. A unit of economic organization or activity especially a business organization.
    b. A systematic purposeful activity agriculture is the main economic enterprise among these people
3. Readiness to engage in daring or difficult action: initiative showed great enterprise in dealing with the crisis

What is Enterprise Risk Management:

We have 2 primary approaches to define Enterprise Risk Management. The first approach being that is defined from the authorities of Enterprise Risk like COSO and ISO. The Second approach is that from the big 4 consulting firms. This would entail what and how these firms would like to classify enterprise risk management.

Enterprise risk according to governing authorities

1. *ISO 31000 Definition*

    According to the International organization of Standardization (ISO)' s document ISO 31000 risk is defined as the effect of uncertainty on an objective. The effect is further defined as deviation from the expected and can be positive, negative, neutral or a combination of all. This effect is either created or is a result of opportunities and threats. It can be addressed.

    Risk

    effect of uncertainty on objectives

    Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

    Note 2 to entry: Objectives can have different aspects and categories and can be applied at different levels.

    Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events their consequences and their likelihood.

Risk management

coordinated activities to direct and control an organization regarding risk[i]

Instead of establishing a rigid definition ISO 31000 is designed to be universally applicable and based on principle standard instead of prescriptive definition.

It outlines how organisations can **integrate risk-based decision-making into their overall governance, planning, management, reporting, policies, values, and culture**.

2. *COSO ERM Definition*

9

Coso Defines ERM as:

The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value.[ii]

The 5 Core Components of COSO ERM

1

The 2017 COSO ERM framework features 20 interconnected principles structured into five primary components:

1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and understanding of risk in the entity.
2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
3. **Performance**: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
4. **Review and Revision**: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and considering substantial changes, and what revisions are needed.
5. **Information**, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Big 4 Definitions and differences

Deloitte: The "Risk Intelligent Enterprise™"

Deloitte defines ERM through its Risk Intelligent Enterprise framework, which places risk and organisational culture at the absolute core of corporate governance.

1. Philosophical Value: Deloitte wants organisations to shift their mindset to balance value preservation (mitigating downside exposures like operational failures and compliance breaches) with value creation (actively taking calculated, strategic risks to drive innovation, market expansion, and business growth).

2. Structural Delivery: Deloitte structures risk governance using the three lines of defence model:

    a. First Line: Business units that actively take and manage risk.
    b. Second Line: Specialized corporate support functions (Finance, HR, IT, Tax, Legal) providing risk infrastructure.
    c. Third Line: Independent internal audit functions delivering objective assurance to the board.
    d. Maturity Curve: They evaluate corporate capability on a risk maturity curve that scales from Initial (Ad Hoc/Fragmented) to Top-Down, Integrated, and ultimately Risk Intelligent.

PwC: Strategic Integration & "Enterprise Resilience"

As a principal co-author of the COSO ERM framework, PricewaterhouseCoopers (PwC) focuses on COSO/ISO harmonization, streamlining internal controls, and building strategic corporate survival systems.

1. Philosophical View: PwC views ERM as a driver of Enterprise Resilience, the holistic capacity of an organisation to anticipate, absorb, adapt, and recover from internal and external shocks. They evaluate and build resilience across three core dimensions; strategic, operational, and financial resilience.
2. Minimum Viable Company (MVC): A signature aspect of PwC's operational model is their Minimum Viable Company (MVC) analysis. This methodology maps an organisation's absolute smallest subset of Critical Business Services (CBS) and assets required to sustain essential operations and protect liquidity during a catastrophic crisis.
3. Technology & Compliance: PwC integrates compliance into product design, using continuous regulatory monitoring and AI-driven platforms (like their "Compliance Insights" SaaS engine) to transform GRC activities from cost centres into strategic capabilities that can reduce Sarbanes-Oxley compliance costs by 25% or more.

EY: Reimagining Risk in the "NAVI" Environment

Ernst & Young (EY) approaches ERM as an agile, real-time operating model designed to navigate the NAVI (Nonlinear, Accelerated, Volatile, Interconnected) risk environment. EY creates a distinction between "Risk Traditionalists" (focused on slow compliance checklists) and "Risk Strategists" (who view risk as an enabler of business growth).

To operate at the "speed of trust" under NAVI conditions, EY designs risk models around three core pillars:

a. Strategy-First: Rather than relying on historical financial loss data or trailing EBITDA to evaluate risk, EY anchors risk priorities, metrics, and appetites in the organisation's strategic projections and future commercial assumptions.
b. Trigger-Based Model: EY advocates moving away from static quarterly or annual risk assessments. Instead, they build continuous monitoring networks that track leading indicators tied to objective trigger thresholds (Monitor, Mitigate, Mobilize), allowing pre-authorized countermeasures to automatically activate the moment conditions shift.
c. Governance-Forward: Accountability, decision rights, and escalation pathways are mapped out and "pre-wired" ahead of time. This allows the board to maintain strict oversight without slowing down executive response times during a crisis.

KPMG: Advanced Analytics and "ERM as a Service"

KPMG's ERM methodology has a highly analytical, quantitative, and mathematical, making it the default choice for heavily regulated, capital-intensive sectors.

1. Philosophical Value: KPMG critiques traditional ERM for relying on slow, two-dimensional "likelihood-and-severity" heatmaps that evaluate risks in isolation. Their argument is that modern risk is systemic and contagious, meaning that risks must be analysed as an interconnected network.

Dynamic Risk Assessment (DRA): KPMG's signature methodology applies network theory, graph mathematics, and expert de-biasing to map risks in four dimensions: Likelihood, Impact, Velocity, and Connectivity.

Consulting Firm	Proprietary Concept	Primary Strategic Objective	Operational Signature
Deloitte	Risk Intelligent Enterprise™	Balancing value preservation with active value creation.	Risk culture assessments and clear board-level governance roles.
PwC	Enterprise Resilience Framework	Protecting organizational survival and optimizing regulatory capital.	Minimum Viable Company (MVC) analysis and compliance automation.
EY	NAVI Risk Transformation	Delivering real-time, strategic decision support.	Strategy-First, Trigger-Based, and Governance-Forward operating models.
KPMG	Dynamic Risk Assessment (DRA)	Uncovering systemic risk connectivity and contagion pathways.	4D network-theory modelling (Likelihood, Impact, Velocity, Connectivity).

Table 1.1: Comparison of Enterprise Risk management within big 4

Chapter II: Case Study

Strategic Enterprise Risk Management: A Capstone Case Study of Zippy.ai

EXECUTIVE SUMMARY & COMPANY PROFILE

In the global logistics sector, which is valued around $39.7 trillion, India is rapidly evolving and growing market currently valued between $135 - $159 billion dollars and estimated to grow up to $300 – 400-dollar billion powerhouse this sector functions as the backbone of India's digital economy. Navigating this complex minefield sector, which is a fast-paced environment with multiple channels and logistic operators becomes a problem for even the most well-established players.

Case Study: Zippyy.ai – Enterprise Risk Management Through Agentic AI

Introduction to Zippyy.ai Zippyy.ai is a native AI-driven logistics operating system and hybrid software/logistics aggregator designed to automate and orchestrate supply chain operations. Founded by leaders with extensive backgrounds in building global enterprise systems, the platform aims to bridge gaps in B2B, B2C, and international shipping by transitioning logistics from reactive, manual operations to predictive, autonomous workflows. Processing over 250 million shipments per month and serving more than 750 brands, Zippyy operates as a top-tier aggregator in the Indian market. By leveraging **Agentic AI** autonomous AI agents that think, decide, and act across logistics workflows Zippyy reduces manual supply chain interventions by up to 70%.

Zippyy.ai is an enterprise which functions as a hybrid service provider, it provides software as a service as well as acts as a logistical operator. They aggregate existing delivery partner information and utilise proprietary technology to help manage shipments by providing the best operator in a particular region for a particular service channel their operations are currently focused on major Indian metro cities specifically Delhi Gurgaon Bangalore and Mumbai.

Zippy.AI has established itself as a critical nodal player that is navigating a landscape which is defined by razor thin margins and hide technological and personal dependency within both the Indian and international ecosystem.

Operational Architecture

Software as a service model:

Zippy.ai provides a sophisticated software as a service which revolves around a robust order management system which utilises Agentic AI as well as machine learning. This architecture synchronises data using API between multiple channel (Amazon and Flipkart, as well as bespoke Direct-to-Consumer (DTC)) storefronts as well as multiple delivery partners (Delhivery, Blue Dart, DTDC among others) in a central dashboard. This dashboard allows

customer to bypass broken workflows as well as make the most informed decision possible and have a more seamless operational layer between sales and Order fulfilment.

Delivery partner:

Utilizes Zippyy's dedicated vehicles and drivers to provide same-day or next-day delivery experiences directly from brand warehouses, bypassing intermediary marketplaces. Traditional quick commerce aggregators (like Blinkit or Zepto) require brands to store their inventory in the aggregator's dark stores or carrier warehouses. For Blue Tokai, this posed a severe operational risk because the quality and smell of roasted coffee degrade every two days. Furthermore, traditional logistics return cycles took up to a week, resulting in ruined, un-sellable inventory. Zippyy eliminated this risk by deploying a dedicated van-based service that collected products directly from Blue Tokai's warehouse. If a customer was unavailable, the coffee remained in the van and was returned to Blue Tokai's warehouse by the end of the same day, radically preserving product integrity and reducing inventory loss.

Competitive Differentiators

Zippy.AI's primary unique selling proposition is that it is an agentic AI driven predictive performance mapping system this significantly reduces return to origin rates which is the single largest cost centre for Indian ecommerce. Whereas traditional aggregators like ship rocket delivery and blue dart primarily focus on shipping rate arbitrage and basic carrier API integration zippy.AI employs an autonomous and predictive performance mapper to protect their margins and merchant return rate.

Zippy.AI's Predictive performance mapper maps logistics partner rating in different areas with order history of customer to calculate order return rate possibility as well as provides the best order fulfilment partner.

Chapter III: Literature Review

Defining the Risk Universe

10 Enterprise risk is defined as the effect of uncertainty on an organization ‘s ability to achieve its objectives to manage this uncertainty we categorise the risk into 4 primary types.

1. Strategic risk: This type of risk that is a threat to the long-term mission market displacement or business model obscene
2. Operational risk: this is the type of risk arising from uncertainty of internal processes human capital or systemic failure including but not limited to supply chain and 3rd party dependency
3. Financial risk: this is the uncertainty related to capital structure liquidity, credit line and defaults
4. Compliance risk: this type of risk can be classified buy legal and regulatory exposures which includes data privacy violation, environmental mandates and other legal compliances

Risk Identification and Risk inventory management

Core Methods of Risk Identification

Under leading frameworks like COSO and ISO risk identification is not a one-time activity but a continuous multidisciplinary exercise. The framework outlines primary approaches to identify risk across enterprise:

1. Interviews: Engaging in one-on-one structured conversation with key employee department heads and SMEs to capture specific exposures in operational compliance and regulatory department as they manage the day-to-day work.
2. Workshops: Gathering cross functional teams in workshops allows for interactive style participation to help find insights and share vulnerabilities and divergent views.
3. Process analysis: Systemic breaking and flow-charting operational workflows to find points of failure and gaps in control activities.
4. Key indicators: Monitoring operational metric and performance deviations to capture warning signs as alerts as alerts before they escalate into incidents and major incidents.
5. Data tracking: Querying historical data like system, audits, other losses to find recurring patterns or cyclical events.
6. Cognitive computing and AI: Leveraging advanced analytics and automation tools to scan vast datasets including external and internal data sets regulatory updates all competitor disclosures to proactively flag emerging risk categories.

Steps to Establish a Comprehensive Risk Inventory

In an effective risk inventory or register. Consolidate identified threats into a structured database that maps how the uncertainties effect the corporate objectives. Establishing this inventory requires a systemic life cycle with the below steps:

1. **Define risk universe and taxonomy:** To ensure consistency, establish a clear hierarchical taxonomy. Categorizing the risk into broad domains and further breaking them into secondary and tertiary categories. To avoid blind spots, apply an exhaustive framework which monitors trends across categories.

2. **Utilise peer group and industry baseline:** Instead of starting from scratch, utilise an inventory compiled by industry associations, regulatory bodies or similarly situated organizations which can then be tailored according to your specific organizational context removing irrelevant risks and adding. Customised or relevant risk unique to your operational footprints and objectives.

3. **Implement Decentralized Risk Ownership:** Establish multi-level risk and compliance committees across different divisions of the company. Clearly delineate roles using a structured accountability framework:

    a. **Risk Owners**: Operational and department managers who are directly accountable for identifying, assessing, and managing risks within their domains.
    b. **Risk Champions**: Dedicated personnel who facilitate regular risk assessments and coordinate the escalation of risk data to the executive risk committee.

4. **Run Horizon Scanning for Emerging Trends:** Emerging risks can be identified by proactively scanning external macro level environments. Government agencies and reputable consulting firms can be leveraged to help identify these emerging risks. Risk managers can shortlist the top x critical trends and map them to concrete impacts on business operations and strategic goals.

5. **Integrate Third-Party Risk Profiles:** Due to modern organizations heavy reliance on external vendor and 3rd party, risk inventory must include exposure from these sites. Performing structured risk and due diligence assessments from time to time on contractors, supplier and partner to update the profiles and risk categorization.

6. **Analyse Interdependencies and Contagion Pathways:** Unlike traditional risk management modern ERM program maps how risks are interconnected. Interdependency focused questions should be embedded into routine assessments and scenario planning exercises. Visual tools like bow tie barrier diagrams and graphs can show how individual minor alerts and triggers can have a cascading effect through systemic domino-effect.

7. **Documenting and Automating the Inventory**: Attempting to manage an enterprise risk register manually using disconnected spreadsheets introduces severe version-control issues and lagging indicators. To build a sustainable program, organizations leverage automated **Governance, Risk, and Compliance (GRC) software**. Centralizing the risk inventory within a GRC database creates a **single, unified risk taxonomy**. This platform automatically maps identified risks directly to their corresponding controls, policies, business units, and strategic objectives delivering real-time risk dashboards that keep C-suite leaders and board committees fully informed.

Core Mitigation Techniques

In capital ERM Once risks are identified and assessed, organization must determine. How to work with them. Under leading framework works risks responses are categorised into 4 core techniques: Mitigation (Reduction), Avoidance, Transference (Sharing), and Acceptance.

1. Risk Mitigation (Reduction): Risk mitigation involves implementing controls, technology or procedural changes to reduce the likelihood and impact of the uncertainty. Here process level controls and forcing functions. (FMEA framework) can be utilised when addressing operational and engineering failures.
    a. Forcing Functions: Introducing physical or administrative constraints that make an error impossible to commit. For example, in healthcare, designing medical gas outlets to only accept matching gauge
    b. Verification Steps: Adding independent double-checks, barcodes, or alert screens to intercept errors before they manifest.
    c. Technological Alerts and Alarms: Using automated monitoring devices to trigger alarms when system values approach unsafe operating limits.
    d. Targeted Redundancy: Installing backup systems (such as backup power generators, firewalls, or flood defences) to mitigate the impact of physical outages.
    e. Behavioural, Training, and Simulation Exercises

Other methods like simulation drills and tabletop exercises war gaming can be utilized to recognize early warning signs or system failure to enable early intervention as well as rehearse response protocols and close preparedness for real world issues. For external disruptions, dual sourcing procurement or keeping buffer stocks can be a good mitigation strategy.

2. Risk Avoidance: Risk avoidance is a strategy where an organization decides not to proceed with an activity or project as the risks associated with those activities exceed the tolerance level for the organization. Examples for these are choosing not to expand operations into a new region or sector or cancelling corporate acquisition after identifying regulatory failure during due diligence or process elimination, like Sunsetting an underperforming or highly vulnerable software system rather than to keep patching it.
3. Risk Transference (Sharing): Risk transference includes shifting a portion of financial or operation risk or consequences with another party. This includes methods like financial hedging. Credit and default mitigation, commercial insurance and captives and outsourcing operations.
    a. Financial Hedging (FX and Commodity Risk): Using derivatives such as forwards and options to lock in exchange rates, thereby protecting profit margins against sudden currency volatility.
    b. Credit and Default Mitigation: Purchasing credit insurance to protect accounts receivable against client default or requiring high-risk customers to provide security via payments in advance, bank guarantees, or letters of credit.
    c. Commercial Insurance & Captives: Transferring liabilities by purchasing specialised coverages (such as cyber liability insurance or property-casualty insurance) or utilizing a captive insurance company.
    d. Outsourcing Operations: Partnering with managed service providers (such as third-party cybersecurity firms) to handle highly complex, high-risk processes that the internal team lacks the capacity to run safely.

4. Risk Acceptance: Risk acceptance is a method where an organization finds the risk. Finds the risk and its impact to be acceptable. Without implementing additional controls or mitigation techniques This may also be as the cost of medication may exceed the potential loss. The methods include passive retention, defining pre-approved financial reserves, active application
    a. Passive Retention (Low-Priority Risks): For minor exposures (such as minor data-entry errors), organisations choose to accept the fallout and resolve errors during routine reconciliation instead of spending capital on automated GRC software.
    b. Defining Pre-approved Financial Reserves: Setting aside designated capital reserves to cover anticipated operational losses while proceeding with high-reward strategic goals.

Mitigation Method	Description	Strategic Trade-off
Transfer	Shifting risk to third parties (e.g., insurance, outsourcing).	Reduces direct exposure but increases third-party dependency and cost.
Avoidance	Exiting high-risk markets or stopping specific activities.	Eliminates the threat but forfeits potential revenue and strategic growth.
Reduction	Implementing internal controls and technology to lower likelihood.	Decreases risk level but requires ongoing capital investment and operational effort.
Acceptance	Retaining the risk within defined appetite thresholds.	Saves mitigation costs but leaves the firm exposed to the full impact of losses.

Table 3.1: Mitigation methods description and trade-offs

Organizations utilize four standard methods to treat enterprise risks, each involving a specific strategic trade-off regarding capital efficiency and residual exposure:

The integration of these methods directly impacts a firm's "Risk Intelligence," determining its ability to maintain stakeholder confidence amidst systemic vulnerabilities. This foundational rigor is particularly critical for the Indian logistics tech sector, where technological complexity and operational velocity create a uniquely high-stakes risk environment.

Formulas to Calculate WHEN to Mitigate Risk

Failure Mode and Effects Analysis (FMEA) – Risk Priority Number (RPN)

Before allocating financial resources, organizations use **FMEA** to mathematically prioritize operational and process-level risks. Teams score three variables on a scale from 1 (best) to 10 (worst):

Severity (S): The severity of the failure's effect on the customer or system.

Occurrence (O): The likelihood or frequency of the failure's root cause materializing.

Detection (D): The likelihood that current process controls will **NOT** detect the failure before it reaches the customer.

$$RPN = S\ x\ O\ x\ D$$

This yields an RPN score between **1 and 1,000**. Generally, organizations establish an action threshold (e.g., any score above **150** or the top 10 highest-scoring risks) that mandates immediate mitigation.

Example: A software feature has a Severity of 8 (critical downtime), an Occurrence of 4 (possible), and a Detection rating of 6 (highly unlikely to be caught prior to release). The calculated RPN is indicating that active mitigation controls are required before release.

Formulas to Calculate HOW MUCH to Invest in Mitigation

To secure budget approvals from executive management, risk leaders must translate technical and operational risks into financial terms.

1. Annualized Loss Expectancy (ALE)

The **ALE** represents the baseline annual monetary loss expected from a specific threat if no mitigation is implemented:

Single Loss Expectancy (SLE): The total financial loss from a single security or operational incident (including direct forensic/remediation costs and indirect customer churn and downtime).

Annualized Rate of Occurrence (ARO): The estimated frequency of the threat occurring within a single year.

$$ALE = SLE\ x\ ARO$$

Example: If an enterprise experiences an average of 10 phishing-origin data breaches per year () and each breach costs $40,000 in recovery and fines (), the baseline **is $400,000**.

2. The Gordon-Loeb 37% Rule (Budget Ceiling)

Developed by cybersecurity economists, this rule establishes the maximum amount an organization should rationally spend on mitigation:

It mathematically demonstrates that due to **diminishing marginal returns**, investing beyond **37% of the expected annual loss** is economically inefficient because the cost of the control will exceed the value of the risk reduction achieved.

$$Mitigation\ Cost \leq 0.3\ x\ ALE$$

Example: With a baseline of $400,000, the maximum economically justified mitigation budget is: Any proposed control costing more than $148,000 is an inefficient use of resources.

3. Return on Security Investment (ROSI)

To prove the concrete financial value of a proposed control to the Chief Financial Officer (CFO), risk leaders calculate the **ROSI**:

M (Mitigation Ratio): The percentage of risk the proposed solution is expected to eliminate (expressed as a decimal, typically between 0.75 and 0.95).

C (Solution Cost): The annual cost to acquire, implement, and maintain the mitigation solution.

$$ROSI = \frac{\big((ALE\ x\ M) - C\big)}{C}\ x\ 100\%$$

Example: Continuing with the $400,000 baseline suppose a data discovery software solution is proposed at an annual cost of $60,000 () with a proven risk mitigation ratio of 94% (). This calculates a **526.6% financial payback**, mathematically justifying the $60,000 investment because it prevents $316,000 in net losses.

Advanced Quantitative Modelling Alternatives

For complex portfolio and compliance exposures, organizations deploy additional statistical calculations:

Value at Risk (VaR): Calculates the expected maximum loss of an asset or portfolio over a set time horizon at a given confidence interval (-score) based on historical volatility ():

$$VAR = V\ x\ (Z\ x\ \sigma)$$

PERT Expected Loss: Used to calculate average expected loss under high uncertainty using a three-point estimation of possible outcomes:

$$Estimated\ Loss = \frac{(Best\ Case + (4\ x\ Most\ Probable\ Case) + Worst\ Case)}{6}$$

COSO Framework

The **Committee of Sponsoring Organizations of the Treadway Commission (COSO)** was originally formed in **1985** as a private-sector initiative. Jointly sponsored and funded by five major professional associations: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA). COSO's core mandate was to improve corporate governance, ethical conduct, and internal control environments.

COSO defines risk simply as **"the possibility that events will occur and affect the achievement of strategy and business objectives"**. This highlights that risk represents both a threat to be mitigated and a potential strategic opportunity to be capitalized on.

The Paradigm Shift: 2004 vs. 2017

COSO released a major revision titled Enterprise Risk Management column, Integrating with Strategy and Performance in 2017. This update marked a critical shift in philosophy.

2004 model: This model used tightly coupled internal controls, audits and backward-looking financial reporting. The original framework categorised risk into 8 distinct components which were internal environments, objective settings, event identification, risk assessment, risk response, control activities, monitoring and information and communication

2017 model: this shift. Redirected ERM from reactive compliance task towards a proactive. Discipline. The modern framework consolidated the 8 activities into 5 core components and 20 guiding principles. This links risk management directly to strategy setting, corporate performance, value creation, Preservation and realization.

The Five Core Components and 20 Guiding Principles

The COSO ERM framework is structured systematically across five interrelated components. Across these components, **20 specific principles** outline what a mature, high-functioning risk capability looks like in practice.

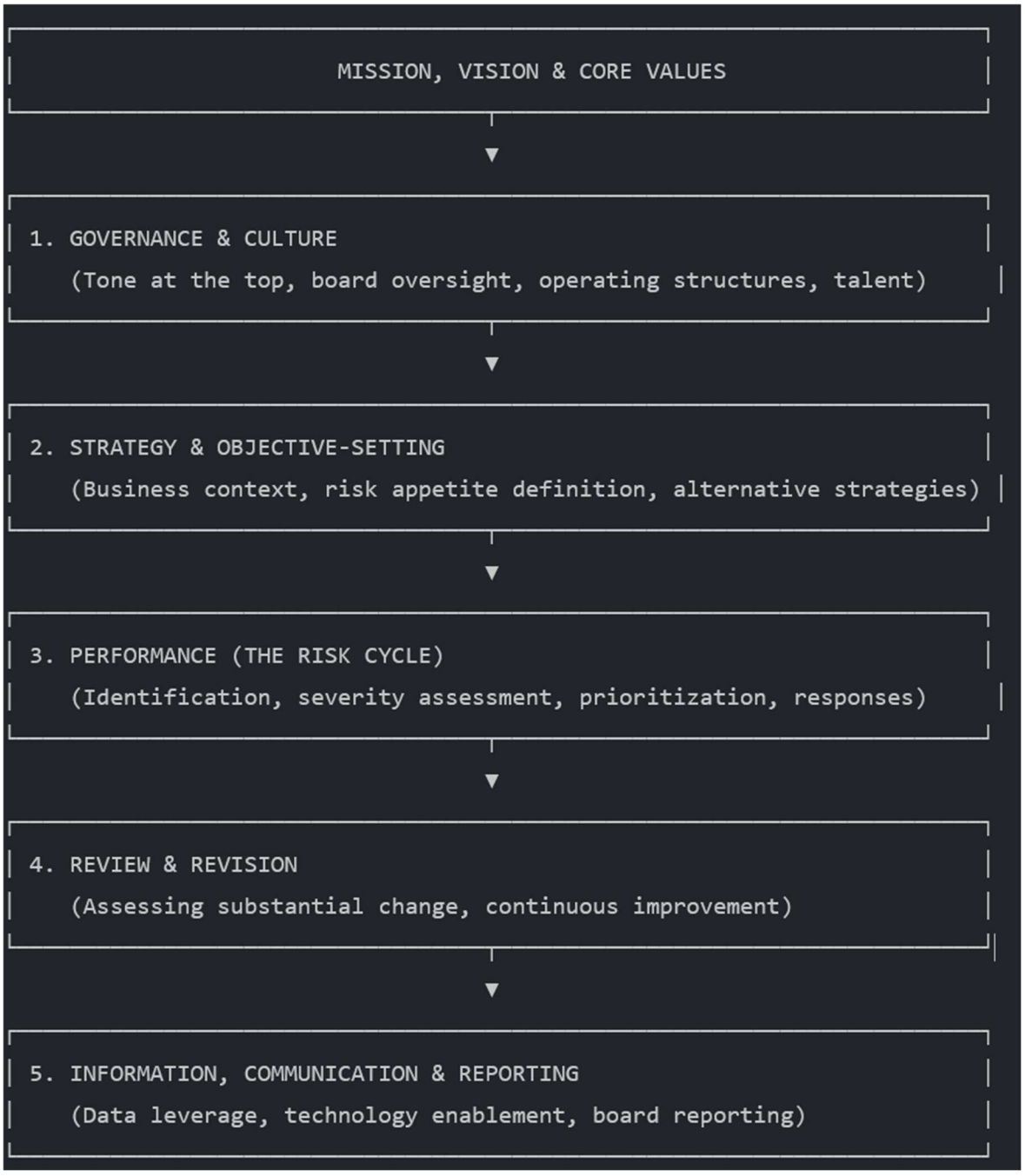


Figure 3.1 : Five Core components of COSO

Principles of COSO model

Governance and Culture

Governance sets the organization stone at the top, and the culture reflects the organization score, value and how employees understand and react to risk. These principles include:

Principle 1 Exercises Board Risk Oversight: The board of directors maintains primary responsibility for risk governance, establishing oversight committees (e.g., Audit or Risk Committees) and reviewing executive strategic risk decisions.

Principle 2 Establishes Operating Structures: Designing clear reporting channels, delegation of authority, and internal compliance hierarchies (e.g., establishing a Chief Risk Officer).

Principle 3 Defines Desired Culture: Cultivating a highly risk-aware culture across all operational departments, ensuring that risk discussions are embedded in daily operating behaviours.

Principle 4 Demonstrates Commitment to Core Values: Aligning company actions with ethical standards, establishing whistleblowing hotlines, protecting whistleblowers, and promoting organizational justice.

Principle 5 Attracts, Develops, and Retains Capable Individuals: Recruiting qualified risk and compliance professionals, conducting risk-based background checks, and linking performance reviews and incentive compensation to risk-aware metrics.

Strategy and Objective-Setting

As ERM operates upstream, COSO argues that risk is an inherent factor in strategy setting. That is, alternate strategies must be evaluated against the organizations risk appetites before the goals are finalized.

Principle 6 Analysing Business Context: Continuous scanning the internal environment (e.g. IT infrastructure) and external environment (e.g. macroeconomic shifts, trade policies, evolving regulations).

Principle 7 Defines Risk Appetite: Quantifying the level and types of risk the organization is willing to accept in strategic pursuit of value.

Principle 8 Evaluates Alternative Strategies: Assessing the risk profiles of different moves (e.g. mergers, product launches) to determine if they align with the board-approved risk appetite.

Principle 9 Formulates Business Objectives: Setting specific, measurable, and achievable targets at each business level, ensuring they carry appropriate risk tolerances.

Performance (The Operational Risk Cycle)

One, strategic objectives are finalised the enterprise must execute core risk management cycles to help identify, prioritize and treat risks.

Principle 10 Identifies Risk: Compiling a comprehensive “risk inventory” of existing, new, and emerging risks across all domains.

Principle 11 Assesses Severity of Risk: Evaluating the likelihood and potential impact of identified threats, leveraging both qualitative matrices and quantitative tools.

Principle 12 Prioritizes Risks: Ranking risks to ensure that corporate resources are directed toward mitigating the most urgent exposures.

Principle 13 Implements Risk Responses: Designing and executing specific risk treatments, categorized into four common paths: **Mitigation** (deploying internal controls), **Avoidance** (cancelling the action), **Transference** (purchasing insurance or outsourcing), or **Acceptance** (retaining minor exposures).

Principle 14 Develops Portfolio View: Stepping back from siloed risk registers to evaluate how different risks across the organization interact and trigger one another.

Review and Revision

Organizations operate in dynamic environments. COSO mandates that the ERM program itself must be continuously audited and revised to prevent it from becoming static.

Principle 15 Assesses Substantial Change: Scanning for major internal and external changes (e.g., leadership transitions; technological breakthroughs like generative AI; or new legislation) that disrupt the risk profile.

Principle 16 Reviews Risk and Performance: Evaluating the actual performance of implemented risk controls to ensure they successfully keep exposures within approved tolerances.

Principle 17 Pursues Improvement in Enterprise Risk Management: Seeking ways to enhance and mature the overall ERM program by conducting self-assessments, benchmarking against peers, and leveraging internal audit reviews.

Information, Communication, and Reporting

Effective risk intelligence requires timely, accurate, and structured data flowing across all levels of the enterprise GRC architecture.

Principle 18: Leverages Information and Technology – Utilizing advanced GRC software, data connectors, and automated workflows to capture risk signals and minimize manual spreadsheet drudgery.

Principle 19: Communicates Risk Information – Ensuring clear, two-way communication channels exist across the “three lines of defence”.

Principle 20: Reports on Risk, Culture, and Performance – Generating tailored dashboards and executive risk reports that translate technical security and operational data into financial terms for the board and C-suite.

ISO Framework

The ISO. 31,000: 2018 Risk management standard. Is a globally recognized principle-based approach to manage the risk uncertainty. Unlike prescriptive frameworks. ISO 31,000 is designed as a flexible philosophy.

The core of the ISO philosophy defines risk as the **"effect of uncertainty on objectives"**. To operationalize this definition, the standard is structured systematically around **three core pillars**: **Principles**, the **Framework**, and the **Process**.

Principles (The Philosophy)

The eight principles form the foundational philosophy of the standard. They dictate what an effective risk management system must be:

1. **Integrated:** It must be an integral part of all organizational activities and processes not a standalone or peripheral concern.
2. **Structured and Comprehensive:** It should define risk management in a clear, systematic, and concise manner applicable across all levels of the enterprise.
3. **Customized:** Practising bodies must tailor their risk management activities to suit their unique operational context, industry, and strategic objectives.
4. **Inclusive:** It requires appropriate and timely stakeholder engagement, capturing diverse perspectives to improve risk awareness.
5. **Dynamic:** The risk system must be highly responsive to change, monitoring for new, emerging, or re-emerging risks as circumstances shift.
6. **Based on the Best Available Information:** Decision-making must rely on historical, current, and projected data, while acknowledging any inherent limitations or assumptions.
7. **Attentive to Human and Cultural Factors:** The standard explicitly recognizes that human behaviours, values, and organizational culture heavily influence how controls succeed or fail.
8. **Oriented Toward Continual Improvement:** The entire risk system must undergo regular reviews, audits, and adjustments to mature over time.

Framework (The Organizational Infrastructure)

The **Framework** defines the organizational structure for embedding risk management into broader corporate governance. It is structured on a continuous improvement cycle based on the **Plan-Do-Check-Act (PDCA) methodology**.

The central point of the framework argues that risk management cannot succeed without active board and C-suite sponsorship. The framework follows a cyclical cycle which is:

At the absolute centre of this framework is **Leadership and Commitment**. ISO 31000 argues that risk management cannot succeed without active board and C-suite sponsorship. Branching out from leadership, the framework follows a cyclic flow:

1. **Integration:** Woven into the governance, structure, and operational rhythms of the organization.
2. **Design:** Designing the overall risk policies, accountability mechanisms, and reporting lines.
3. **Implementation:** Executing the risk program across decentralized business units.
4. **Evaluation:** Systematically assessing the effectiveness of the risk management program.
5. **Improvement:** Adapting and enhancing the framework to align with newly emerging threats.

Because of the structure ISO 31000 functions. As a layer which can seamlessly integrate with other ISO standards such as 9001 for quality 14001 for environment and 27001 for information security without forcing organizations to maintain redundant or competing architecture.

Process (The Operational Execution)

While the Framework establishes the infrastructure, the **Process** outlines the exact operational steps required to systematically identify, analyse, and manage risks on the ground:

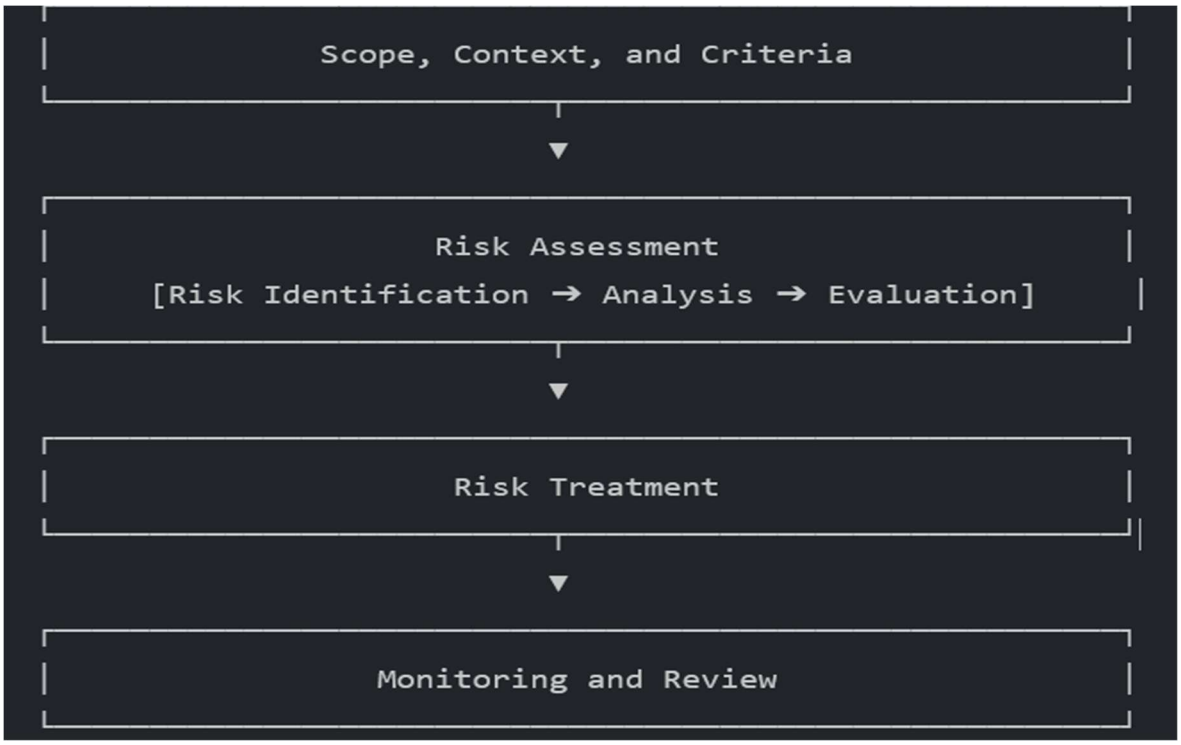


Figure 3.2: Framework for ISO Process

Recording, reporting, communication & Consultation occurs continuously across all steps

1. **Scope, Context, and Criteria:** This is the first step which establishes the boundaries of assessment, maps out both internal and external environments, and defines specific risk criteria.
2. **Risk Assessment:**
    a. *Risk Identification:* Compiling a detailed risk inventory of threats that could prevent objective achievement.
    b. *Risk Analysis:* Calculating risk severity by assessing the likelihood and consequences of events, taking existing controls into consideration.
    c. *Risk Evaluation:* Comparing the analysed risk levels against the established criteria to prioritize which threats require immediate action.
3. **Risk Treatment:** In this step we select and execute Response options like avoidance, mitigation, transfer, or acceptance.
4. **Monitoring and Review:** Continually evaluating if risks remain within acceptable tolerances and checking if control activities perform as designed.
5. **Recording and Reporting:** Creating a transparent audit trail of risk documentation and reporting outcomes to the board.

6. **Communication and Consultation:** Ensuring continuous, bidirectional feedback and open dialogue with stakeholders at every single phase of the process.

Importance of Enterprise Risk Management

Modern ERM has transitioned from a defensive, checkbox compliance exercise into a vital strategic step that directly helps in driving corporate values, operational resilience and competitive advantages. Within the corporate environment implementing a mature ERM framework is critical for several reasons:

1. **Direct Improvement of Financial Performance and Value Creation:** As a core value, every business to. Protect the value it creates for its stakeholders. Academic research validates that proper risk management is a performance lever:
    a. A comprehensive review of 212 academic papers reveals that 68% of research findings demonstrate a statistically significant positive relationship between ERM implementation and corporate performance.
    b. Sound ERM adoption is directly correlated with improvements in core metrics such as Tobin's Q (firm market value) and Return on Assets (ROA).
    c. Properly managed ERM programs help secure optimized financing terms and a lower cost of capital. Listed firms utilizing ERM experience a 1% to 3% lower cost of capital than those without.
    d. Implementing ERM reduces earnings volatility and market shock impacts, leading to a significant decline in the standard deviation of stock returns.

2. **Strategic Growth and Opportunity Enablement:** Unlike traditional risk management, which was historically a defensive hazard mitigation and loss preventor modern ERM is a proactive strategic enabled that helps in value creation and preservation. It systemically aligns the organisations risk appetite and tolerance with the organization's strategic goals and objectives. This alignment empowers senior leadership and boards to make risk-adjusted decisions. By clearly defining what level of uncertainty the organization is willing to accept, leaders can confidently pursue strategic opportunities (such as mergers, acquisitions, and technological innovations) to drive growth.

3. **Elimination of Silos and Holistic Risk Visibility:** Removal of silos and having a more holistic approach allows modern ERM to have a more cohesive enterprise wide. Portfolio view instead of. Individual departments of sectors. It provides a structured framework to identify and manage the interlinking of risks across different types of risk and departments. The risk is volatile. In nature. And rarely occurs in isolation, instead. They operate as a complex network which can. Have a domino effect. ERM helps visualize how a single operational vulnerability can cascade across different

business units. This helps prevent critical risk from slipping through the gaps between organizational silos and prevents misallocation of resources.

4. **Operational Agility and Outage Prevention:**
5. In modern day fast paced environment, traditional risk management which was slow calendar driven assessments cannot help providing real time decision supports:
    a. Proper ERM establishes **leading Key Risk Indicators (KRIs)** tied directly to risk appetite thresholds. These metrics act as proactive "tripwires" that provide early warnings of potential threats before they escalate into crises.
    b. Organizations that actively link risk and strategy (known as "Risk Strategists") demonstrate far greater resilience. They report a **reduced proportion of unexpected risks** and exhibit **significantly faster incident identification and response times** than traditionalist companies.
    c. Leveraging GRC technology to automate these risk registers and compliance workflows drives substantial efficiency, yielding **50%-to-80%-time savings** and up to **60% in compliance cost savings**.

6. **Strengthened Governance, Compliance, and Stakeholder Trust:** The Sea- Suite and Board of Directors have explicit fiduciary duties to oversee corporate risk and safeguard company assets, implementing a formal ERM framework. Is a fundamental step of corporate governance:
    a. ERM provides the robust documentation and auditable workflows required to satisfy strict regulatory reporting demands (such as Sarbanes-Oxley, ESG double materiality guidelines, and industry-specific solvency capital requirements).
    b. Proactively demonstrating a rigorous risk management system **builds deep credibility and trust** with external stakeholders, including credit rating agencies, lenders, regulators, customers, and investors. This strong reputation acts as an organic safeguard to protect overall corporate brand value.

Chapter IV: Analysis

The Top Five Emerging Risks Landscape (2Q26)

According to Gartner 's report of 2Q 2026 the top 5 highest aggregate ranked risk score items are:

1. AI Discovery of Cyber Vulnerabilities (Risk Score: 3.76)
2. Geopolitical Energy Supply Shocks (Risk Score: 3.49)
3. Agentic AI (Risk Score: 3.41)
4. Information Integrity Risk (Risk Score: 3.40)
5. AI Workforce Preparedness Gap (Risk Score: 3.36)

Score Rank	Risk Name	Impact Score	Time Frame Score	Frequency
1	AI Discovery of Cyber Vulnerabilities	3.22	1.92	76%
2	Geopolitical Energy Supply Shocks	2.83	1.64	61%
3	Agentic AI	2.80	2.25	69%
4	Information Integrity Risk	2.72	1.94	64%
5	AI Workforce Preparedness Gap	2.70	2.35	72%

Figure 4.1: Gartner top 5 risk rank with impact and frequency score

According to Gartner’s 2Q26 Emerging Risk Report (the latest data compiled in June 2026), AI Discovery of Cyber Vulnerabilities risk secured the #1 rank globally with an aggregate Risk Score of 3.76 and was selected by 76% of surveyed risk leaders as a top ten concern.

The rapid rise of this threat is fueled by three main drivers

1. Widespread growth and uncoordinated growth of autonomous AI tools: Malicious actors and automated systems are deploying AI tools that independently scanning, identifying, and exploiting system vulnerabilities at scale, accelerating discovery far beyond manual oversight capacities.
2. Rapid Exploit Creation: The gap between vulnerability discovery and defense is collapsing because AI enables near-instant, automated exploit deployment, expanding high-level attack capabilities beyond elite hackers to average threat actors.
3. Increased System Complexity: The massive enterprise push to integrate AI into daily workflows has dramatically increased software architectural complexity, limiting visibility and making real-time remediation at scale highly difficult.

Potential Consequences for Enterprises

If left unmitigated, this AI discovery of vulnerabilities introduce severe operational and financial vulnerabilities:

1. Backlogs of Unpatched Vulnerabilities: AI-powered discovery outpaces the capacity of IT security teams to write, test, and deploy patches, creating dangerous backlogs of critical, exposed vulnerabilities.
2. Loss of Sensitive Data and IP: The accelerated speed of exploitation increases the likelihood of unauthorized network access, which exposes sensitive Personally Identifiable Information (PII) and corporate intellectual property.
3. Escalating Security Costs: Organizations face severe budget strains from rising cyber insurance premiums, potential regulatory fines (under frameworks like GDPR or DORA), and diminished returns on AI investments.
4. It is defined as the risk of rapid advances in AI accelerating the discovery and exploitation of previously unknown (zero-day) cyber vulnerabilities, outpacing organizational defenses, leading to cascading cyber incidents and operational disruptions.

Macro Risk Context: Gartner Research on Agentic AI

According to Gartner 's emerging risk report of 2026 agentic AI is ranked 3 among the top emerging global risks with a risk score of 3.41 and an impact score of 2.80 additionally, agentic AI was also ranked number one in potential business opportunity in the Q4 2025 Organizations leverage autonomous AI agent execute both simple and complex task automation. Gartner’s 2026 CIO survey indicates that 81% of CIOs plan to deploy AI agents from 2026 to mid-2027 with 17% already starting rollout.

Gartner Bow-Tie Root Cause & Impact Mapping for Agentic AI



Figure 4.2: Gartner Bow tie Root cause and impact mapping

Gartner bow tie method Uses a visual Diagram like a bow tie to link Root cause of risk to its potential consequences. For the impact of agent tech AI. Gartner defines agentic AI risk as the threat of autonomous agents' execution decision ability that deviates from organizational policies, ethical standards. Or legal mandates which can cause operational compliance, reputational or financial harm. The root causes for the same are:

1. **Unclear Governance & Lifecycle Controls:** Done governance for agentic AI across its design deployment and execution in real life scenarios with real time monitoring.
2. **Third-Party & Shadow Agent Proliferation:** Unmonitored Or ungoverned integration of AI agents across. SaaS tools, partner platforms with fragmented oversight.
3. **Memory-Poisoning Vulnerabilities:** Exploitation of an agent's long-term memory buffer through corrupted inputs or prompt injections, distorting reasoning pathways.

Cascading Consequences: For agentic AI, the cascading consequences. Include triggering of unauthorised financial transactions, modification Off parameters as well as taking actions where the threshold value has not reached to take the action.

Zippy.ai Dilemma: Agentic Autonomy vs. Human-in-the-Loop

Zippy.AI has deployed a specialized agentic AI. Which allows for inventory and fulfilment agent to help automate order fulfilment, carrier allocation and merchant query. This Implementation of agentic AI covers multiple risk factors from Gartner 's top 5 emerging. Risk report. Including but not limited to agentic AI actions, AI workforce preparedness gap, AI discovery of cyber vulnerabilities as well as information integrity risk which will come as a cross-scope risk from agentic AI itself.

One of the potential risk event scenarios may be:

The Human-in-the-Loop (HITL) Threshold Control

- **Confidence Gating:** Zippy sets a strict mathematical threshold for its agents. If an agent's evaluation score falls below **0.8** (or if the risk score exceeds 0.8), automated execution is blocked, and the transaction escalates to a human operator for manual review.
- **85% HITL Retention:** For routine, low-risk queries (e.g., simple inventory lookups), the system responds automatically. However, for high-stakes decisions involving monetary transactions, contract execution, or carrier switching, Zippy enforces an **85% Human-in-the-Loop requirement**.

The Risk Event Scenario

Due to corrupt data corruption or malicious injection into the memory of Zippyy's fulfilment agent, thus manipulating the confidence level to be different than the actual value which can bypass the human in the loop or trigger human in the loop when not required this can cause delays or financial, operational and reputational consequences like the agent

autonomously cancels thousands of shipments with primary carrier Delhivery and reallocates them to a higher-cost, unverified third-party carrier. This triggers:

- **Operational Fallout:** Massive shipment backlogs, delayed deliveries, and broken merchant SLAs.
- **Financial Fallout:** Unexpected surge charges, margin compression, and breach of contractual volume commitments with Delhivery.
- **Compliance & Data Privacy Fallout:** Exposure of e-commerce customer Personally Identifiable Information (PII) to unauthorized third-party logistics entities.

Integrated ERM Framework Coupling (COSO + ISO 31000 + NAVI)

To govern high-velocity threats like Agentic AI, Zippy.ai can pair COSO ERM (2017) with ISO 31000:2018

1. Dual-Path Framework Hybridization
    a. COSO ERM at Board Level: Provides the structural scaffolding for board-level risk oversight, risk appetite definition, and strategy alignment across 5 components and 20 principles.
    b. ISO 31000 at Operational Level: Provides a flexible, Plan-Do-Check-Act (PDCA) process loop used by engineering and supply chain teams to conduct real-time risk assessments across decentralized hubs.

2. AI Governance via NIST AI RMF 1.0
    a. Implementation of an AI governance like NISTAIR MF 1.0 can be useful to help mitigate as well as monitor the impact risks associated with AI. The implementation of the framework across Zippyy's agent life cycle would include:
    b. Govern: Establish an AI risk committee to define the acceptable AI risk criteria and tolerance as well as create policies to track accountability for autonomous decision making.
    c. Map: Document all dependencies input output potential impact across logistic workflows for the AI agent.
    d. Measure: Implement measurable benchmarks for the 7 characteristics of trustworthy AI like validity safety resilience transparency and fairness.
    e. Manage: Deploy active risk responses, including continuous prompt sanitization, memory-buffer resets, and automated fallback routines.

3. Business Continuity via PwC's Minimum Viable Company (MVC)
    a. Using PwC's MVC methodology, Zippy identifies its Critical Business Services (CBS) specifically, order ingestion, carrier rate calculation, and label generation.

b. In the event of an Agentic AI collapse or major carrier API outage (e.g., Delhivery API downtime), Zippy's MVC protocols activate a pre-programmed failover mechanism that automatically reroutes order volumes to secondary carriers (BlueDart/DTDC) using deterministic static rate cards, preserving core operational continuity.

4. Data Protection & Continuous Control Monitoring (CCM)
   a. To maintain compliance with India's Personal Data Protection Act (PDPA), Zippy transitions from point-in-time annual audits to Continuous Control Monitoring (CCM) using GRC platforms (such as UnderDefense MAXI).
   b. CCM automatically ingests security telemetry, validates encryption of customer PII across API endpoints in real time, and generates audit-ready compliance proof without manual intervention.

5. Operationalizing EY's NAVI Strategy
   a. In this high-speed AI driven environment traditional reviews like annual or quarterly are ineffective therefore zippy can try and adopt e wise 3 Navi pillars:
   b. Strategy first: zippy can directly tie strategic projections to risk tolerances rather than financial metrics this would allow zippy to make decision based more on risk and strategic objectives rather than financial games which will take time and are slow.
   c. Trigger base model: instead of calendar driven reviews uh trigger beige reviews will allow for faster and more comprehensive understanding and handling of risks and its consequences these triggers can include:
      i. *Monitor:* KRIs track prompt anomaly rates, agent hallucination metrics, and carrier API latency.
      ii. *Mitigate:* If agent confidence scores fluctuate between 0.70 and 0.80, the system automatically forces a mandatory secondary human approval step.
      iii. *Mobilize:* If unauthorized agent actions breach A certain cumulative or if memory poisoning is detected, pre-authorized playbooks instantly freeze autonomous execution and revert all shipping logic to deterministic rule-based algorithms or human in the loop.
   d. Governance forward: decision making, escalation an executive authority during AI crisis should be pre hardwired into the system to eliminate decision latency.

6. Financial Risk Controls & Working Capital Optimization
   a. To protect against credit default risks from small Direct-to-Consumer (DTC) brands, Zippy optimizes its Cash Conversion Cycle (CCC):

b. Zippy enforces a prepaid wallet architecture for high-risk DTC merchants. Shipping fees are automatically deducted from pre-funded merchant wallets prior to label generation, driving DSO toward zero and insulating Zippy from bad debt write-offs.

Chapter V: Conclusion

Zippy has is small but impactful risk with when it comes to financial control and working capital optimization which it can mitigate mostly by optimising its cash conversion cycle and enforce a prepaid wallet architecture 4 direct to consumer merchants.

Due to its heavy reliance on technology the next risk which carries medium impact would be related to data protection and business continuity due to technological issues. For both risk profiles zippy must update its security as well as keep alternatives in case of loss of communication due to API or technological issues with other supplying operators.

The highest risk and its impact for zippy dot AI comes from the agentic implementation. Due to this being an emerging technology and having very few safeguards this risk carries the most catastrophic consequences to zippy.AI. To navigate this risk zippy must lead in agentic AI governance framework as well as change their risk calculation time from a timeline to a trigger mechanism. Technologically, Zippyy operates on a threshold-based Agentic AI model to balance automation with risk. While low-hanging operational tasks are fully automated, complex decisions generate a confidence score. If the AI's confidence falls below a 0.8 threshold, or if the action involves high-stakes financial or personnel decisions, the system enforces a "human-in-the-loop" requirement. Currently, approximately 85% of complex tasks retain human oversight to ensure trust and accuracy.

11

[i] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[ii] https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf