Entreprise risk management

Foly Ananou, PhD

Course objectives

- Master ERM fundamentals : understand the principles, frameworks, and benefits of ERM
- Analyse and measure risk: learn to identify risk, assess and quantify risks using qualitative and quantitative tools
- Understand the implementation of ERM and best practices

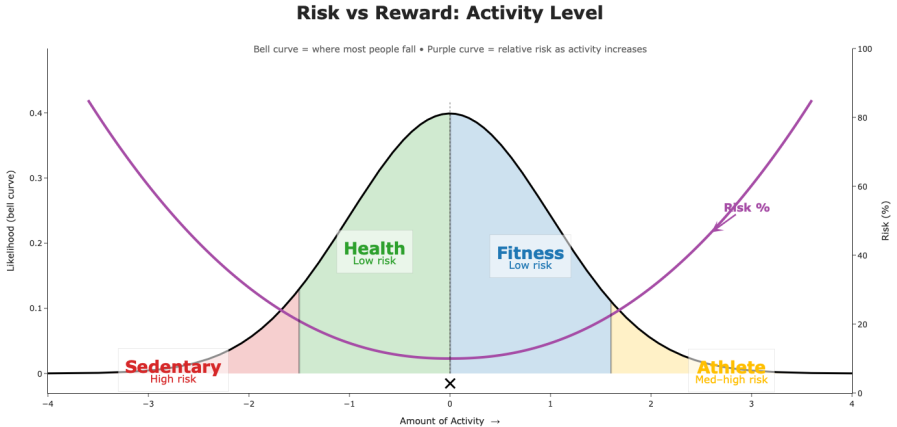
ERM: fundamentals

Understanding risk: preview

- Let consider the following situations:
  - You are in vacation in Cote d'Ivoire and decide to have an outdoor gathering with friends at the beach. $\rightarrowtail$ What could possibly go wrong ? How likely could this happen ? if it does happen, will it be very harmful ? What can you do to prevent the event from happening or reduce the impact ?
  - You got it involve in a car crash $\rightarrowtail$ Is it necessary someone fault or is it just one of those things that happen in life ?

Understanduing risk: a definition

- Berstein (1996) defines risk as the uncertainty around the outcome of a decision, process or event which can be negative (losses) or positive (benefits or opportunities).



Understanduing risk: key characteristics of risk

- Uncertainty : outcomes are not guaranteed or predictable
- Dual nature: risk is not only about threats or losses, it can also includes opportunities
- Measurable dimensions:
  - **exposure** $\rightarrowtail$ what is at stake ?
  - **probability** $\rightarrowtail$ how likely is it possible ?
  - **severity** $\rightarrowtail$ how bad (or good) coud it get ?
  - **time** $\rightarrowtail$ how long ?
  - **correlation** $\rightarrowtail$ can it escalate or drive other risks ?

Understanduing risk: categorization

- Can you identify the risk type in the following sceenarios ? (let guess together)
  - A large international bank experiences a sophisticated ransomware attack that encrypts critical customers data and shuts down online banking services for almost 2W.
  - The government announces overnight that all cryptoccurrencies transactions are banned taking effect immediately, forcing fintech companies to halt operatiions immediately.
  - An investment firm relies heavily on a proprietary risk model to allocate capital. During a period of market stress, the model significantly underestimates correlations across asset classes, leading to losses far exceeding management's stated risk appetite.
  - An extreme weather event severely damages key production facilities of an energy company, forcing a prolonged shutdown. At the same time, regulators announce tighter environmental standards, increasing future compliance and investment costs.

Understanduing risk: categorization

- There is no "one-size-fit-all" in terms of risk category : it's dependent on the analysis framework.
  - Market risk can be related to financial markets, for firms it could relate to their ability to compete in a given (chosen) market(s)
  - Business risk can indicate the full scope of risks faced by a firm or just a subset (specific) risk related to the type of business the firm is envolved in (insurance risk for example)
  - Credit risk can include or exclude risk of changes in observed market credit spread – with some hint also to liquidity risk.

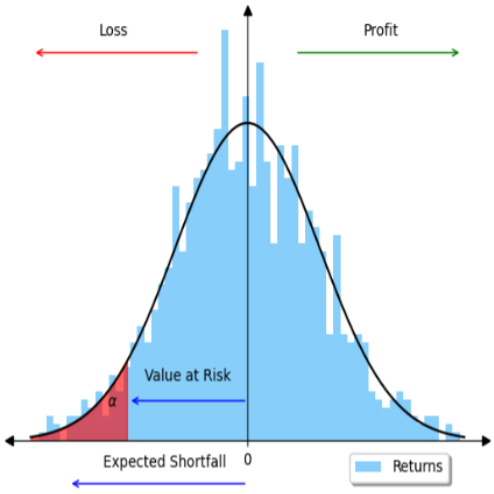
Understanduing risk: financial risk (credit, liquidity and interest-rate)

- A bank lends money to firms and households, and its funding is essentially based on customers deposits.
  - In what situations does the bank lose money ?
    - Total or partial ? Why ?
    - Will the losses occur immediately or over time ?
  - In what situation does the bank run out of cash ?
    - Does that mean the bank is insolvent ?
    - Can the bank fail in that situation ?
  - In what situation does the bank profit fluctuate even there is nothing wrong on its customers side ?
    - The bank makes 20-year fixed-rate loans at 2%. It funds itself with deposits whose interest rate can change every year. What happen if interest rate rise to 5% ?

Understanduing risk: financial risk (credit, liquidity and interest-rate)

- Commonly used and simplest measures are the Value-at-risk (VaR) and Expected Shortfall (ES)
  - VaR summarizes potential financial losses within a firm, portfolio, or position over a specific time frame. It reflects the worst expected loss under a given time horizon ...
    ...given a certain confidence level.
  - Expected shortfall extends VaR by capturing tail risk beyond the VaR cutoff.

VaR and ES exercices



Definition of ERM

- Lam (2003) "ERM is all about integration: ... an integrated risk organisation, ... the integration of risk transfer strategies, ... the integration of risk management into the business process of a company"
- Kemp and Patel (2011) define ERM as a framework, using risk as the core building block, to enable key business decisions to be aligned with inherent riskIt involes hoslistic management of risk and management of business/portfolio as an enterprise.
- Casualty Actuarial Society (2003) "The discipline by which and organization in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the organization's short and long-term value to its stakeholders."

Discussion: Does ERM create value for a firm ? Why and how ?

Evolution of ERM

- ERM has evolved from a control-oriented function to a strategic framework focused on value creation.
  - **Compliance and risk control** : Initial focus on regulatory compliance and adherence to limits, with risks managed in silos.
  - **Loss minimisation** : Emphasis on reducing downside outcomes through basic mitigation tools and operational controls.
  - **Risk management** : Development of structured risk identification, assessment, and mitigation processes across the organization.
  - **Risk measurement** : Introduction of quantitative tools such as economic capital models, stress testing, and scenario analysis to measure risk consistently.
  - **Strategic integration (today)** : Integration of risk considerations into strategic decisions, capital allocation, and performance management.
  - **Risk optimisation and value creation** : State-of-the-art ERM treats risk as a resource to be actively allocated in order to optimise risk–return trade-offs and support long-term value creation.

Core risk terminology

- **Uncertainty** : Lack of complete information about future outcomes, without necessarily implying measurable probabilities.
- **Risk exposure** : The degree to which the organization is subject to a given risk, given its activities, assets, and environment.
- **Risk appetite** : The amount and type of risk an organization is willing to accept in pursuit of its strategic objectives.
- **Risk tolerance** : Acceptable variation around objectives, translating risk appetite into operational limits.
- **Risk capacity** : The maximum level of risk the organization can absorb without threatening its viability.
- **Residual risk** : The level of risk remaining after controls and mitigation actions are applied.
- **Inherent risk** : The level of risk that exists in the absence of any controls or mitigation.

ERM Framework

- **Reference frameworks (COSO, ISO 31000)** : Provide a common structure and language for identifying, assessing, and governing risks across the organization.
- **Risk principles and policies** : Establish consistent rules for how risks are defined, assessed, reported, and escalated.
- **Risk appetite and tolerance** : Translate strategic objectives into explicit limits on acceptable risk-taking and risk variability.
- **Link to strategy and performance** : Ensure that risk considerations influence strategic choices, capital allocation, and performance evaluation.

ERM Architecture

- **Board of Directors**
  Sets risk appetite, oversees risk strategy, and ensures that risk-taking is aligned with the organization's long-term objectives.
- **Risk Committee**
  Provides focused oversight, challenges management decisions, and ensures timely escalation of material risks.
- **Executive Management**
  Owns risk-taking decisions and integrates risk considerations into day-to-day management and strategic planning.
- **Chief Risk Officer (CRO)**
  Provides an independent, enterprise-wide view of risk and coordinates risk management activities across functions.
- **Three Lines of Defense**
  Clarifies roles between risk-taking (first line), risk oversight and control (second line), and independent assurance (third line).

ERM process

Identify : Identify potential risks that could affect objectives

Monitor: Continuously monitor risks and the effectiveness of strategies

Assess: Evaluate to understand impact and likelihood

Communicate: Ensure stakeholders are informed about risks and management activities

Manage and respond: Develop strategies to address identified risks

Discussion: Is ERM a quantitative or a qualitative tool ?

ERM: Framework, Architecture and Process (synthesis)

Framework Defines principles, boundaries, and acceptable risk-taking (risk appetite, policies, strategic alignment).

Architecture Allocates responsibilities and ensures risk oversight (board, CRO, three lines of defense).

Process Operationalizes ERM through identification, assessment, response, and monitoring of risks.

Synthesis

Effective ERM requires consistency between what is allowed (framework), who is accountable (architecture), and how risks are managed (process).

Cases studies: why ERM fails ?

Why ERM Fails in Practice (synthesis)

- ERM failures typically reflect governance and judgment issues rather than technical deficiencies.
  - **ERM reduced to compliance**
    Frameworks exist formally but do not influence strategic decisions.
  - **Unclear or ineffective risk appetite**
    Limits are vague, ignored, or overridden during growth phases.
  - **Misaligned incentives**
    Short-term performance is rewarded while risk accumulation is not penalized.
  - **Weak challenge and escalation**
    Risk signals are diluted, delayed, or dismissed when inconvenient.
  - **Illusion of control through models**
    Quantitative tools create false confidence and mask tail risks.

Key takeaway

ERM fails when risk governance is disconnected from decision-making, incentives, and organizational culture.

ERM frameworks and architecture

ERM Frameworks: What problem do they Solve?

Organizations face many risks simultaneously, across units, time horizons, and objectives.

ERM frameworks exist to solve three coordination problems:

- **Cognitive problem:** Different actors perceive and describe risk differently.
- **Organizational problem:** Risks are generated locally but consequences are enterprise-wide.
- **Governance problem:** Risk-taking decisions are often separated from risk-bearing consequences.

Core function

An ERM framework aligns perception, responsibility, and decision-making around risk.

COSO ERM: Why the control orientation?

COSO ERM emerged from repeated failures in financial reporting and governance.

- The primary concern is **accountability**: who is responsible when objectives are missed?
- Risk is framed as a **source of deviation** from expected outcomes.
- Emphasis is placed on documentation, traceability, and auditability.
- The framework assumes that better controls reduce unacceptable risk.

Implicit assumption

Risk failures are largely due to weak controls or poor oversight.

COSO ERM: Where the logic breaks

The control-based logic has structural limits.

- Not all risks are controllable ex ante (strategic, systemic, tail risks).
- Excessive controls can delay decisions and suppress risk signals.
- Documentation may substitute for genuine challenge.
- Strategic risk-taking can be discouraged even when value-creating.

Key insight

Strong controls do not guarantee good risk decisions.

ISO 31000: Risk as a Decision Problem

ISO 31000 starts from a fundamentally different premise.

- Risk is defined as the **effect of uncertainty on objectives**, not merely as potential loss.
- Risk management is meaningful only if it influences decisions.
- There is no universally optimal risk process — context matters.
- Judgment is unavoidable and must be structured, not eliminated.

Implicit assumption

Risk cannot be fully controlled, only understood and governed.

ISO 31000: Why flexibility becomes a weakness

Without strong governance, ISO-based ERM can drift.

- Risk appetite remains qualitative and non-binding.
- Different units interpret principles inconsistently.
- Risk discussions lack escalation and enforcement.
- Strategic narratives replace quantitative discipline.

Failure mode

Risk is discussed but not constrained.

COSO ERM vs ISO 31000: Two philosophies of ERM

- **COSO ERM**
  - **Primary logic: accountability and control** – Designed to reduce deviations from objectives through clear governance, internal control, and traceability.
  - **Strength: auditability and discipline** – Produces roles, documentation, and evidentiary trails that work well in regulated or listed environments.
  - **Typical failure mode: compliance substitution** – When treated as a checklist, the firm may appear "in control" while strategic and tail risks remain unchallenged.
- **ISO 31000**
  - **Primary logic: decisions under uncertainty** – Risk is the effect of uncertainty on objectives; ERM help shape choices, trade-offs, and priorities.
  - **Strength: integration and flexibility** – Principles-based design encourages embedding risk into strategy, planning, and day-to-day decisions across diverse contexts.
  - **Typical failure mode: dilution and inconsistency** – Without strong governance, principles can become vague, unevenly applied, and non-binding for risk-taking.

Takeaway

COSO $\rightarrowtail$ *discipline, controls, and assurance* are the priority; ISO $\rightarrowtail$ *decision integration and strategic adaptation* are the priority.

Risk apetite: How it works in practice

Risk appetite is a **governance mechanism**, not a slogan.

- It translates strategic ambition into acceptable uncertainty.
- It constrains risk-taking before losses materialize.
- It provides a reference for escalation and challenge.
- It must be expressed in both qualitative and quantitative terms.

Key mechanism

Risk appetite defines when risk-taking becomes a governance issue.

Confusing Appetite, Tolerance and Capacity is dangerous

These concepts play different roles in ERM.

- Risk appetite reflects **strategic choice**.
- Risk tolerance reflects **operational control**.
- Risk capacity reflects **survival constraints**.

- Exceeding tolerance requires management action.
- Exceeding appetite signals strategic drift.
- Exceeding capacity threatens viability.

Crisis pattern

Most failures occur when appetite silently converges toward capacity.

ERM Maturity models: The hidden trap

ERM maturity models suggest linear progress.

- They implicitly assume that more integration is always better.
- They reward formalization over effectiveness.
- They can encourage cosmetic improvements.
- They underestimate the role of context and strategy.

Key warning

High ERM maturity does not immunize against failure.

Why ERM frameworks become box-ticking

Box-ticking is a rational organizational outcome.

- Framework adoption is often driven by regulation or reputation.
- Incentives favor formal compliance over substantive challenge.
- Responsibility for risk is diffused.
- Negative information is costly to escalate.

Structural insight

Box-ticking is not a mistake — it is a governance failure.

What Makes an Effective ERM Framework?

- An effective ERM framework is not the presence of documents; it is a system that **changes decisions** and **constrains risk-taking** before losses occur.
  - **Clear objectives and risk taxonomy** – Risks are defined relative to objectives, using a common language that avoids silo interpretations and enables aggregation at enterprise level.
  - **Explicit risk appetite linked to strategy** – Appetite expresses the acceptable uncertainty required to pursue strategy; it becomes meaningful when translated into operational limits and triggers.
  - **Decision-usefulness (not reporting volume)** – Risk information must answer: *What changes in our decision today?* Otherwise ERM becomes descriptive rather than prescriptive.
  - **Escalation and consequence mechanisms** – Effective frameworks define when issues must be escalated and what actions follow (reduce exposure, revise limits, halt activity, strengthen controls).
  - **Balance of quantitative and judgment** – Models structure discipline; judgment handles regime shifts, tail risks, and what data cannot capture.

Litmus test

If risk appetite breaches do not trigger action and debate at the right level, the framework is cosmetic.

Transition: From Framework to Architecture

A framework specifies **what should happen**. Architecture determines **who makes it happen** and **how power and information flow**.

- **Who owns risk? (risk-taking authority)**
  Business units typically originate risk; architecture clarifies the limits of their autonomy and when decisions become governance issues.
- **Who challenges risk? (independent oversight)**
  The CRO and second-line functions must have independence, access, and standing to challenge decisions that conflict with appetite or capacity.
- **Who assures risk controls? (independent assurance)**
  Internal audit validates that controls and reporting are effective, not only present, and that exceptions are properly managed.
- **How escalation works under pressure**
  Architecture defines escalation paths that still function when incentives push toward ignoring bad news.