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

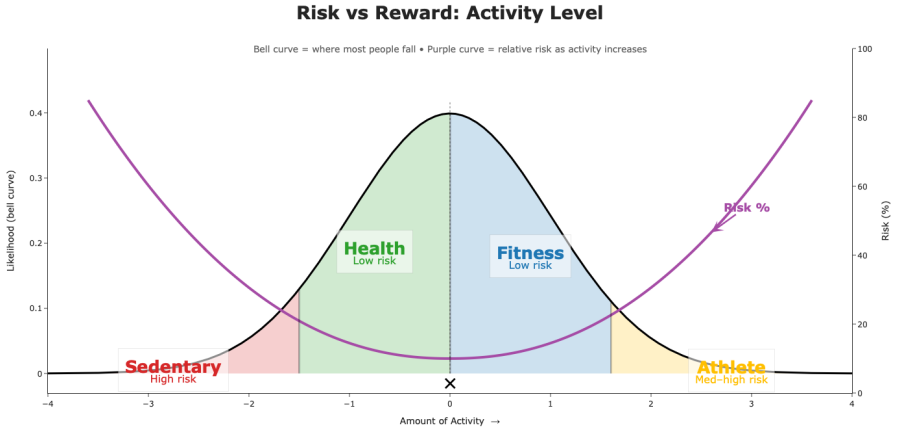
ERM: fundamentals

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.

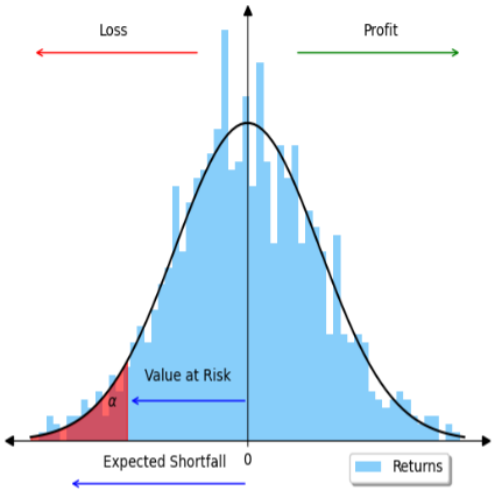
Understanduing risk: financial risk (credit, liquidity and interest-rate)

- 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 (recap)

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).