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

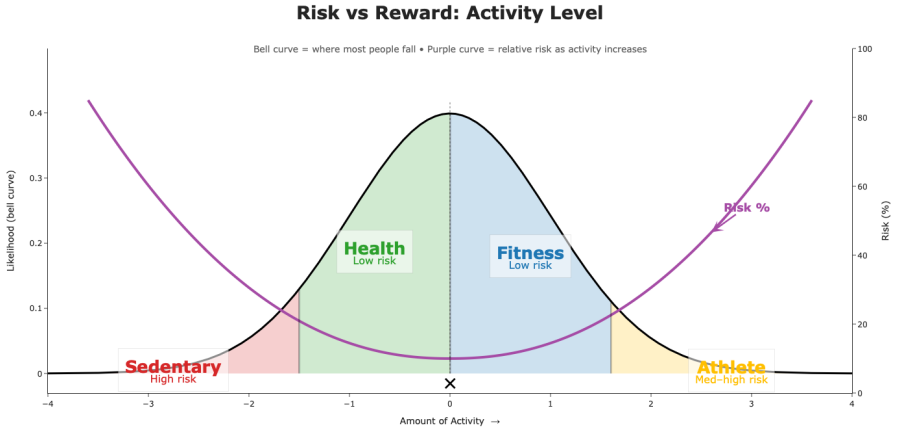
ERM: fundamentals

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.

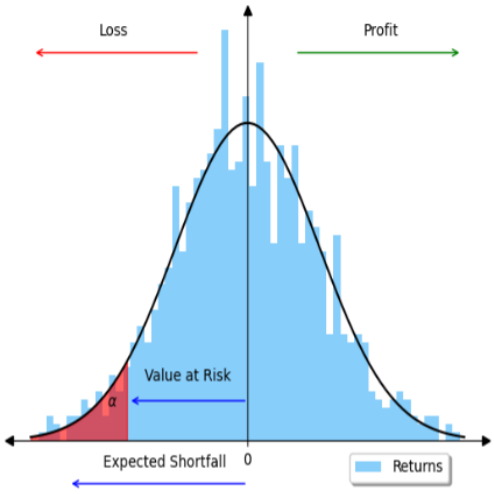
Understanduing risk: financial risk (credit, liquidity and interest-rate)

- 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.

Practice



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).

Practice

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.

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.

ERM Architecture: Core functions

ERM architecture is a governance system that performs four critical functions.

- **Allocation of decision rights**
  Determines who can take risk, within which limits, and under what conditions.
- **Independent challenge**
  Ensures that risk-taking decisions are reviewed and contested by actors without direct profit incentives.
- **Information and escalation**
  Guarantees that material risks reach the appropriate decision level in time.
- **Assurance and accountability**
  Verifies that controls work and assigns responsibility when outcomes diverge.

Organizing principle

Architecture is about enforcement, not reporting.

Decision rights and Risk-taking

Risk originates from decisions, not models.

- Business units make local decisions that generate enterprise-wide risk exposure.
- Risk-taking authority is delegated but constrained by mandates, limits, and escalation triggers.
- When decision rights are implicit or informal, risk accumulates outside governance boundaries.

Failure pattern

Most risk is taken where governance is weakest.

Independent challenge and oversight

Effective ERM requires structured disagreement.

- The CRO provides an enterprise-wide perspective and challenges business decisions that conflict with appetite.
- Independence is necessary but insufficient; influence and access to decision-makers are equally critical.
- Challenge fails when it is perceived as advisory rather than consequential.

Key tension

The CRO has responsibility without direct authority.

Information flow and escalation

ERM architecture lives or dies through escalation.

- Risk information must travel upward without filtering, delay, or strategic framing.
- Escalation thresholds define when risk becomes a governance issue rather than an operational one.
- Escalation mechanisms must still function when incentives push toward silence.

Diagnostic test

Would bad news still be escalated if it threatened careers?

Assurance and accountability

Controls without assurance create an illusion of safety.

- Internal audit independently verifies the effectiveness of risk controls and reporting.
- Assurance focuses on whether controls work in practice, not whether they exist on paper.
- Clear accountability strengthens incentives to respect limits and escalation rules.

Common mistake

Auditing processes instead of risk outcomes.

ERM Architecture under pressure

ERM architecture is revealed when conditions deteriorate.

- Growth phases weaken constraints and encourage overrides.
- Stress exposes information bottlenecks and authority gaps.
- Weak architectures fail silently before losses appear.

Final takeaway

Architecture determines whether ERM constrains behavior or merely documents it.

ERM architecture in banks: why it is specific

Banking ERM architecture is shaped by the interaction between risk-taking, capital, and financial stability.

- Banks operate with **high leverage**, making small shocks potentially systemic rather than firm-specific.
- Risk-taking decisions directly affect **capital adequacy**, liquidity, and solvency.
- ERM architecture must therefore satisfy not only shareholders, but also **supervisors and the financial system**.

Key implication

In banks, ERM architecture is inseparable from regulation and supervision.

Basel framework as an architectural constraint

The Basel framework embeds risk constraints into bank governance.

- Capital requirements limit the amount of risk that can be absorbed by the balance sheet.
- Risk-weighted assets translate heterogeneous risks into a common capital metric.
- Liquidity and leverage ratios constrain funding structures and balance sheet expansion.
- These constraints shape risk-taking incentives before management discretion intervenes.

Architectural role

Basel rules act as ex ante enforcement of risk appetite at system level.

ICAAP: linking ERM to capital and stress

The Internal Capital Adequacy Assessment Process (ICAAP) is the core internal ERM mechanism in banks.

- ICAAP translates the bank's risk profile into internal capital needs under normal and stressed conditions.
- It forces management to articulate assumptions about risk, correlations, and tail events.
- Stress testing within ICAAP reveals vulnerabilities not captured by standard risk metrics.
- ICAAP connects risk appetite, capital planning, and strategy.

Failure pattern

ICAAP fails when it becomes a regulatory document rather than a decision-making tool.

Resolution and SRB: architecture under failure

ERM architecture in banks extends beyond survival scenarios.

- Resolution frameworks assume that banks can fail and design mechanisms to contain systemic impact.
- The Single Resolution Board (SRB) evaluates resolvability and loss-absorbing capacity.
- ERM must therefore consider not only risk prevention, but also **orderly failure**.
- Risk-taking inconsistent with resolvability constraints undermines the credibility of ERM.

Architectural insight

In banking, ERM must be credible even in failure.

Synthesis: banking ERM as layered enforcement

- Basel sets system-wide minimum constraints.
- ICAAP internalizes risk into capital planning.
- Governance bodies arbitrate trade-offs.
- Resolution frameworks discipline excessive risk-taking.

Key takeaway

Banking ERM architecture is effective only when regulatory, internal, and governance layers reinforce each other.

Risk culture: the missing enforcement layer

Formal architecture cannot fully constrain behavior.

- Risk culture shapes how individuals interpret rules, limits, and escalation thresholds.
- It determines whether risk signals are amplified or suppressed within the organization.
- Culture becomes decisive when rules are ambiguous or incomplete.

Lam's insight

Risk culture determines how ERM functions when no one is watching.

Incentives and risk-taking behavior

Incentives translate abstract objectives into concrete behavior.

- Compensation structures influence risk-taking more powerfully than formal policies.
- Short-term performance incentives encourage risk accumulation that may only materialize later.
- Poorly designed incentives weaken escalation and encourage limit overrides.

Behavioral mechanism

People manage what they are rewarded for.

Tone from the top and challenge culture

Leadership behavior sets the effective risk boundary.

- Tone from the top signals whether risk management is valued or tolerated.
- A strong challenge culture allows disagreement without career penalties.
- Silence in meetings often reflects incentives, not consensus.

Diagnostic question

Are people rewarded for raising inconvenient risk concerns?

Why ERM still fails despite strong architecture

Even robust ERM architectures can collapse.

- Incentives overpower formal constraints.
- Escalation is perceived as costly or futile.
- Success reinforces overconfidence and risk drift.

Final takeaway

ERM fails when incentives and culture neutralize governance.

Practice

ERM and decision-making

Why risk-adjusted performance metrics exist

Accounting performance measures ignore the uncertainty underlying returns.

- Two activities can generate identical profits while exposing the organization to very different downside risks.
- Risk-adjusted performance metrics explicitly relate expected returns to the amount of risk or capital required to sustain them.
- Their primary function is to make heterogeneous activities comparable from a decision-maker's perspective.

Decision purpose

Risk-adjusted metrics enable ranking and allocation, not prediction.

RAROC and EVA: what they measure and why they exist

RAROC and EVA are economic performance metrics designed to link risk, capital, and value creation.

- **RAROC (Risk-Adjusted Return on Capital)** measures the expected return of an activity relative to the amount of economic capital required to absorb unexpected losses. It answers the question: *How much return do we earn per unit of risk-bearing capacity consumed?*
- **EVA (Economic Value Added)** measures value creation by comparing operating profits to the full cost of capital, including the opportunity cost of bearing risk. It answers the question: *Does this activity create value once risk is fully priced?*
- Used together, RAROC supports **relative ranking and capital allocation**, while EVA supports **value creation assessment** at firm or business-unit level.

Important clarification

RAROC and EVA structure decision-making under uncertainty; they are not precise valuation tools.

ERM as a strategic discipline

Strategy is inseparable from risk-taking.

- Strategic choices determine which risks the organization deliberately accepts in pursuit of value.
- ERM makes these choices explicit, coherent, and consistent with risk-bearing capacity.
- When conditions change, ERM provides the basis for revising strategy rather than reacting after losses materialize.

Final insight

ERM is effective when it shapes strategy ex ante, not when it explains failures ex post.

Why risk-adjusted decision-making still fails

Even when risk-adjusted metrics are available, decisions may ignore them.

- Incentives may favor short-term accounting performance over risk-adjusted value creation.
- Portfolio effects and correlations may be underestimated, leading to excessive concentration.
- Model assumptions may understate tail risks, especially during benign periods.
- Governance may allow exceptions that neutralize discipline.

Link to ERM

Risk-adjusted metrics require architecture, incentives, and culture to be effective.

Exercise 1: risk-adjusted performance and allocation

A bank considers three business activities competing for limited capital. Expected annual figures are shown below.

	Activity A	Activity B	Activity C
Expected profit (€m)	12	9	6
Economic capital (€m)	60	30	15

The bank has a total economic capital budget of €75m and a target RAROC of 15%.

1. Compute the RAROC of each activity.
2. Rank the activities based on their risk-adjusted performance.
3. Given the capital constraint, which activities should the bank prioritize?
4. Is it optimal to select only the activity with the highest RAROC? Explain.
5. How does this exercise illustrate the role of ERM in capital allocation?

Exercise 2: portfolio view and strategy

The bank currently operates Activity B and Activity C from Exercise 1. Management considers adding Activity A to boost profitability.

Additional information:

- Activity A and B are exposed to the same economic sector.
- Activity C is weakly correlated with A and B.
- Under adverse conditions, losses on A and B tend to materialize simultaneously.

The bank's stated strategy emphasizes resilience and stable earnings.

1. From a standalone perspective, does Activity A appear attractive? Why?
2. How do correlation and concentration change the risk assessment at portfolio level?
3. Why might a portfolio-level perspective contradict the RAROC ranking?
4. Is the proposed expansion consistent with the bank's stated strategy?
5. What additional information would ERM require before approving this decision?

ERM and core risk categories

Credit risk in ERM

Credit risk is the risk of loss arising from counterparty failure.

- Traditional credit risk focuses on probability of default and loss given default at individual exposure level.
- From an ERM perspective, concentration, correlation, and cyclicality are often more dangerous than isolated defaults.
- Credit risk interacts strongly with market conditions, liquidity, and strategy during downturns.

ERM role

Ensure credit growth, portfolio concentration, and capital planning remain consistent with risk appetite.

How ERM governs credit risk hedging

ERM governs credit risk hedging as a portfolio and capital decision.

- **Risk appetite and scope:** ERM determines which credit risks are core to the business model and should be retained, and which exposures (e.g. sectoral or single-name concentration) should be reduced.
- **Hedging instruments:** ERM guides the use of collateral, guarantees, credit insurance, credit default swaps (CDS), securitization, or portfolio sales depending on objectives.
- **Portfolio focus:** Hedging targets correlation, concentration, and tail exposure rather than individual defaults.
- **Secondary risks:** ERM assesses counterparty risk, liquidity risk, basis risk, and legal risk introduced by credit hedges.
- **Governance:** Limits are set on hedge reliance, counterparty exposure, and complex structures, with escalation for exceptions.

ERM principle

Credit hedging arbitrates risk transfer versus capital usage at enterprise level.

Market risk in ERM

Market risk arises from changes in prices, rates, and spreads.

- Day-to-day volatility is usually manageable and expected.
- The main ERM challenge lies in tail events, correlation breakdowns, and forced deleveraging.
- Market risk becomes systemic when combined with leverage and liquidity constraints.

ERM role

Prevent market risk from amplifying into solvency or liquidity crises.

How ERM governs market risk hedging

Market risk hedging balances volatility reduction with liquidity and strategy.

- **Risk tolerance:** ERM defines acceptable earnings volatility and tail losses, which determines the extent of hedging.
- **Hedging instruments:** Forwards, futures, swaps, options, and structured derivatives are used to reshape exposure profiles.
- **Hedging design:** ERM distinguishes between linear hedges (cost-efficient) and optional hedges (tail protection).
- **Secondary risks:** ERM evaluates margin calls, liquidity needs, basis risk, and counterparty exposure arising from hedges.
- **Governance:** ERM limits speculative hedging, complexity, and model-dependent strategies.

ERM principle

Market hedging reduces volatility but must preserve liquidity and resilience.

Operational risk in ERM

Operational risk arises from failures in processes, systems, people, or governance.

- Operational risk is often treated as residual, but it frequently triggers or amplifies other risk categories.
- Weak controls, poor data, or governance failures can turn manageable risks into severe losses.
- Culture, incentives, and decision processes are key drivers of operational risk.

ERM role

Identify structural weaknesses that cut across all risk categories.

How ERM governs operational risk mitigation

Operational risk is mitigated primarily through governance and controls.

- **Risk identification:** ERM identifies critical processes whose failure could amplify financial or strategic risks.
- **Instruments and tools:** Insurance contracts, outsourcing agreements, redundancy systems, and business continuity plans.
- **Control design:** ERM prioritizes investments in systems, controls, and data quality based on risk materiality.
- **Secondary risks:** ERM evaluates dependency risk, legal risk, and residual exposure not covered by insurance.
- **Governance:** Clear accountability and reporting lines are enforced for operational incidents.

ERM principle

Operational risk mitigation improves how the organization functions.

Liquidity risk in ERM

Liquidity risk arises when obligations cannot be met without severe cost.

- Liquidity risk materializes abruptly and is highly non-linear.
- It often results from interactions between market stress, funding structures, and confidence.
- Liquidity crises frequently occur despite compliance with other risk limits.

ERM role

Ensure that growth, leverage, and funding strategies remain resilient under stress.

How ERM governs liquidity risk mitigation

Liquidity risk is governed structurally rather than hedged transaction by transaction.

- **Risk tolerance:** ERM defines survival horizons and stress scenarios under which liquidity must be preserved.
- **Instruments and tools:** High-quality liquid assets (HQLA), committed credit lines, central bank facilities, and funding diversification.
- **Structural constraints:** ERM constrains maturity transformation, leverage, and reliance on short-term funding.
- **Secondary risks:** ERM assesses rollover risk, collateral availability, and market access under stress.
- **Governance:** Contingency funding plans and escalation protocols are embedded in ERM.

ERM principle

Liquidity resilience is achieved through structure, not derivatives.

Strategic risk in ERM

Strategic risk arises from flawed assumptions, choices, or execution.

- Strategic risk is forward-looking and often difficult to quantify.
- It reflects misalignment between strategy, environment, and risk-bearing capacity.
- Most major failures are strategic in nature, even if losses appear as credit or market losses.

ERM role

Challenge strategic assumptions and test resilience under alternative scenarios.

How ERM governs strategic risk

Strategic risk is governed through flexibility and disciplined choice.

- **Risk framing:** ERM challenges strategic assumptions using scenarios and stress testing rather than point forecasts.
- **Instruments and mechanisms:** Real options, staged investments, exit clauses, diversification, partnerships, and joint ventures.
- **Irreversibility control:** ERM limits commitments that could lock the organization into fragile strategies.
- **Secondary risks:** ERM evaluates reputational, political, and long-horizon risks created by strategic choices.
- **Governance:** Strategic decisions are subjected to explicit risk challenge at board level.

ERM principle

Strategic risk is reduced by preserving optionality, not by eliminating risk.

Risk categories are not silos

Enterprise risk emerges from interactions.

- Credit stress can trigger market losses and liquidity runs.
- Operational failures can magnify all other risks.
- Strategic errors often determine the scale of losses.

Key message

ERM exists to arbitrate interactions, not to optimize silos.

Derivatives in ERM: why they are ubiquitous

Derivatives are the dominant instruments for hedging because they allow precise and flexible risk transfer.

- Derivatives isolate specific risk factors (rates, prices, spreads, FX) without requiring changes to the underlying business activity.
- They enable rapid adjustment of exposures, which is particularly valuable when risks evolve faster than balance sheets.
- Compared to structural changes, derivatives are often capital-efficient and operationally convenient.
- However, derivatives do not remove risk from the system; they transform it into counterparty, liquidity, model, and governance risks.
- As a result, derivative usage is not a technical decision but an enterprise risk decision.

ERM perspective

Derivatives are powerful risk-shaping tools, but they require strict governance to avoid amplifying enterprise risk.

Hedging assessment

ERM assesses hedging both *before* and *after* implementation.

- **Unhedged and hedged positions:** Let X denote the unhedged exposure and H the hedging instrument. The hedged position is defined as:

$$Y = X - hH$$

  where h is the hedge ratio chosen by the firm.

- **Hedge ratio (definition):** The hedge ratio represents the quantity of hedging instrument used per unit of exposure. A common benchmark is the minimum-variance hedge ratio:

$$h^* = \frac{\mathrm{Cov}(X, H)}{\mathrm{Var}(H)}$$

  used as a reference rather than a mechanical rule in ERM.

Hedging assessment

- **Prospective effectiveness (ex ante):** ERM evaluates whether the hedge is expected to reduce risk:

$$\mathrm{HE}_{\mathrm{pros}} = 1 - \frac{\mathrm{Var}(Y)}{\mathrm{Var}(X)}$$

  based on assumptions about correlation, volatility, and stress scenarios.

- **Retrospective effectiveness (ex post):** After implementation, ERM reassesses realized performance:

$$\mathrm{HE}_{\mathrm{retro}} = 1 - \frac{\mathrm{Var}(X - hH)}{\mathrm{Var}(X)}$$

  to detect model drift, breakdowns, or unintended risk amplification.

Hedging assessment

- **ERM extension to tail risk:** Effectiveness is also assessed on downside risk:

$$\Delta ES = ES(X) - ES(Y)$$

  complemented by analysis of liquidity and margin impacts.

ERM interpretation

A hedge is acceptable only if prospective and retrospective effectiveness remain robust under stress and do not create secondary enterprise risks.

Practice

ERM in practice

Why ERM implementation is structurally difficult

ERM implementation fails not because principles are unclear, but because it conflicts with how organizations actually operate.

- ERM requires coordination across functions that are traditionally autonomous (finance, risk, business, strategy).
- Risk considerations often impose constraints on growth, leverage, or profitability, which creates natural resistance.
- The benefits of ERM are probabilistic and long-term, while the costs (foregone opportunities, additional controls) are immediate.

Implementation insight

ERM is difficult because it changes incentives and power, not because it lacks tools.

Common ERM failure modes

Many organizations formally adopt ERM while neutralizing its impact.

- **Box-ticking ERM:** risk registers and policies exist, but they are disconnected from actual decisions.
- **Risk reporting without consequence:** dashboards are produced, but no action follows deterioration.
- **Over-measurement:** excessive metrics dilute attention and create a false sense of control.
- **Fragmentation:** risk categories are managed in silos, preventing portfolio-level insight.

Diagnostic

ERM fails when it produces information but does not alter behavior.

Deeper failure modes: incentives and governance

The most damaging ERM failures originate in incentive structures.

- Performance evaluation emphasizes short-term accounting outcomes rather than risk-adjusted or long-term value.
- Business units are rewarded for growth and volume, while risk functions bear responsibility without authority.
- Exception processes become systematic, undermining formal limits and risk appetite.
- Risk signals are softened or delayed as they move up the hierarchy.

ERM reality

Risk cannot be governed if those who take risk do not bear its consequences.

ERM as a change management problem

Implementing ERM requires altering how decisions are proposed, challenged, and approved.

- Managers must justify decisions not only in terms of return, but also in terms of risk and resilience.
- ERM introduces structured challenge, which can be perceived as loss of autonomy or trust.
- Without visible support from top management, ERM is easily bypassed or marginalized.

Key condition

ERM succeeds only when senior leadership actively uses it in decisions.

Integrating ERM into strategic planning

ERM must shape strategic choices rather than react to them.

- Strategic plans should explicitly state key risk assumptions about markets, funding, regulation, and technology.
- Scenario analysis should test strategy robustness under adverse but plausible conditions.
- ERM should identify which strategic options are fragile versus resilient across scenarios.

Strategic test

Would this strategy still be acceptable if key assumptions fail?

Integrating ERM into budgeting and forecasting

Budgeting is a critical but often neglected ERM entry point.

- Budgets typically reflect optimistic point forecasts rather than distributions of outcomes.
- ERM introduces downside scenarios and stress assumptions into revenue, cost, and funding projections.
- Risk appetite should constrain budgeted growth, leverage, and concentration.

Implementation rule

If budgets ignore downside risk, ERM is not embedded.

ERM in capital allocation and investment approval

Capital allocation is where ERM becomes binding.

- Investment proposals should include risk-adjusted performance metrics and stress outcomes.
- ERM enables comparison of projects with different risk profiles competing for limited capital.
- Projects that are profitable in expectation may be rejected if they increase fragility at portfolio level.

Decision logic

ERM shifts the focus from isolated profitability to portfolio resilience.

Dashboards: role and common pitfalls

Dashboards are often overestimated as ERM solutions.

- Dashboards summarize information but do not create discipline by themselves.
- Excessive indicators dilute attention and mask deterioration.
- Backward-looking metrics provide comfort rather than early warning.

Key insight

Dashboards support ERM only when linked to escalation and action.

Designing dashboards that support ERM

Effective ERM dashboards are selective and forward-looking.

- Indicators should be explicitly linked to risk appetite and strategic objectives.
- Trends, concentrations, and stress metrics are more informative than point estimates.
- Visual design should make deterioration immediately visible, without interpretation.

Design principle

If escalation thresholds are not obvious, the dashboard fails.

Reporting, escalation, and accountability

Information without accountability does not reduce risk.

- ERM reporting should define clear thresholds that trigger mandatory discussion or action.
- Responsibilities for response must be explicit and documented.
- Failure to escalate should itself be treated as a risk event.

ERM mechanism

ERM works when risk signals force decisions, not explanations.

What makes ERM work in practice

- ERM must be embedded in planning, budgeting, and capital allocation.
- Incentives and authority must be aligned with risk ownership.
- Tools and dashboards support judgment but do not replace it.

Final takeaway

ERM succeeds when it systematically changes how decisions are made under uncertainty.

ERM across industries: four mini cases

- Same ERM principles, different industry economics.
- Each case is designed for diagnosis: identify ERM design, what failed, and why.
- Focus on interactions: risk categories, instruments, governance, incentives.

Group task

For each case: (i) identify the dominant risks and their interaction, (ii) infer ERM architecture, (iii) explain failure modes, (iv) propose 1–2 ERM improvements.

Mini case: financial institution — Silicon Valley Bank (SVB)

SVB's business model was highly concentrated in technology startups and venture capital clients. Deposit growth surged in the low-rate period, with a deposit base dominated by large, uninsured corporate balances that were highly confidence-sensitive. The bank invested a substantial share of excess deposits into long-duration fixed-income securities (Treasuries and agency MBS). While credit risk was limited, the duration exposure created substantial interest rate risk as rates rose in 2022–2023.

As market values declined, unrealized losses accumulated. Risk measurement and regulatory reporting existed, but ERM did not translate these signals into binding decisions. Hedging of interest rate risk was reduced rather than increased, partly to preserve short-term earnings. Liquidity stress testing did not fully reflect the speed and concentration of outflows possible in a networked depositor base. When concerns surfaced, withdrawals accelerated rapidly and the interaction between interest rate losses, liquidity pressure, and confidence dynamics resulted in a rapid bank run and failure.

SVB: questions for diagnosis

1. Which risks were central (interest rate, liquidity, concentration, confidence)? How did they amplify each other?
2. What ERM elements likely existed (limits, ALM, stress tests, governance) and where did they fail to affect decisions?
3. Why can compliance and measurement coexist with failure? Identify the decision points that should have changed.
4. What would an ERM redesign prioritize: deposit concentration governance, hedging policy, escalation, or incentives?

Mini case: energy and commodities — Metallgesellschaft (1993)

Metallgesellschaft, via its U.S. subsidiary, offered long-term fixed-price contracts for petroleum products, creating long-horizon exposure to commodity price changes. To hedge, it built a large futures position in short-dated oil contracts and rolled them over time. Economically, the hedge aimed to offset long-term price risk using a dynamic futures strategy.

The design was vulnerable to liquidity stress. As prices moved against the futures position, variation margin outflows surged. Even if the hedge could work economically over the long run, it required short-run funding capacity to survive adverse moves. Management underestimated the scale and persistence of margin calls and the governance needed to manage liquidity and unwind risk. The interaction between market risk, liquidity risk, and governance led to forced unwinds at losses, turning a hedging program into an enterprise-level crisis.

Metallgesellschaft: questions for diagnosis

1. Why can a hedge be economically rational yet operationally fragile? Identify the key mechanism.
2. Which enterprise risks were created by the hedge (liquidity, basis, governance, model dependence)?
3. What hedging assessment should ERM have required (stress margin funding, survival horizon, escalation)?
4. Propose an ERM-compliant redesign: instruments (options vs futures), limits, funding buffer, governance.

Mini case: non-financial corporation — Boeing and the 737 MAX

Boeing operates in a safety-critical industry where operational and reputational risks dominate financial hedging logic. The development of the 737 MAX took place under intense competitive pressure and strong time-to-market constraints. Key design and certification choices emphasized speed and cost containment. Safety risks related to new flight control functionality were not escalated effectively, and internal challenge mechanisms proved weak. Formal risk processes and compliance structures existed, but they did not constrain strategic and operational decisions. After two fatal accidents, the aircraft was grounded globally, producing severe financial losses, reputational damage, and long regulatory scrutiny. The episode illustrates how ERM can fail primarily through governance, culture, and incentives, even when risks are knowable and procedures exist.

Boeing: questions for diagnosis

1. What were the dominant risk families (operational safety, strategic, regulatory, reputational)?
2. Where did ERM fail: identification, escalation, challenge, or incentive alignment?
3. What signals should have triggered escalation, and why might they have been filtered or ignored?
4. Propose two ERM architecture changes that increase challenge power without paralyzing innovation.

Mini case: public sector and infrastructure — megaproject risk

Large public infrastructure projects (rail, transit, airports) face long horizons, multiple stakeholders, political oversight, and high public visibility. Initial project approval often relies on optimistic forecasts for costs, timelines, and demand. Even where formal risk frameworks exist, downside risks are systematically underestimated because incentives favor launching projects and because accountability is diffuse.

As implementation proceeds, technical complexity, regulatory changes, procurement frictions, and stakeholder opposition compound initial underestimation. Risk registers may document risks, but ERM frequently lacks authority to halt projects, force major redesign, or credibly escalate bad news. The result is a pattern of cost overruns, delays, and legitimacy loss. The case highlights that in the public sector, the core ERM challenge is often governance and incentive compatibility rather than measurement.

Megaprojects: questions for diagnosis

1. Why do public projects tend to exhibit optimism bias and weak downside planning?
2. How do political incentives and diffuse accountability constrain ERM effectiveness?
3. What should an ERM escalation mechanism look like when decision rights are political?
4. Propose an ERM design that introduces credible challenge (stage gates, independent review, stop rules).

Cross-case synthesis: what differs, what remains

- Financial institutions: small shocks can threaten solvency/liquidity; models and capital are central, but governance is decisive.
- Energy/commodities: derivatives are powerful, but margining and liquidity can dominate outcomes under stress.
- Non-financial corporations: ERM is mainly governance, escalation, and culture; technical risk is often not the binding constraint.
- Public sector: ERM is constrained by politics and accountability; challenge must be institutionalized through process and independence.

Unifying insight

ERM succeeds when it changes decisions under uncertainty and fits the organization's incentives and constraints.

Comparison matrix: architecture, instruments, typical failure

Industry	Typical ERM anchor	Frequent failure mode
Financial institutions	Capital, liquidity, stress tests, board risk governance	Model comfort + ignored signals; liquidity run dynamics
Energy & commodities	Hedging policy + liquidity buffers + scenario culture	Margin spiral; basis/correlation breakdown; weak governance
Non-financial corporates	Governance, escalation, culture, controls	Incentives dominate; bad news filtered; safety/quality subordinated
Public sector & infrastructure	Stage gates, independent review, accountability	Optimism bias; weak stop rules; political override

Practice

Ten common myths about enterprise risk management

- ERM eliminates risk rather than managing risk-taking.
- More data and more models necessarily improve decisions.
- Risks can be fully understood through quantitative metrics.
- Hedging always reduces enterprise risk.
- ERM is primarily a compliance or regulatory requirement.
- Risk ownership can be delegated to a risk function.
- Scenario analysis is a substitute for judgment.
- Dashboards prevent surprises.
- A well-designed ERM system cannot fail.
- ERM failures are always due to lack of information.

Final message

ERM succeeds not by predicting the future, but by shaping decisions under uncertainty.