R53 Introduction to Risk Management

Version 1.0

1. Introduction

Investors often assume higher risk in the pursuit of higher returns. Businesses and investors manage risk, whether consciously or not, in every investment decision they make. This reading lays the fundamentals of risk management from the perspective of both businesses and individuals.

Some of the important concepts addressed in this reading include:

- What is risk management and why is it important?
- How businesses and individuals manage risk?
- The principles behind both enterprise and portfolio risk management.
- How an entity's goals are affected by risk and how risk management decisions produce better results?
- Identifying the various risks and the tools used by an organization to manage risk.

2. The Risk Management Process

Risk is the exposure to uncertainty. Risk driver is the underlying risk. Risk position is the description or quantification of the risky action taken. Risk exposure is the extent to which an entity is sensitive to underlying risks. In other words, risk exposure is the risk position multiplied by the risk driver.

Risk management is the process by which an organization or individual defines the level of risk to be taken (risk tolerance), measures the level of risk being taken (risk exposure), and adjusts the latter toward the former, with the goal of maximizing the company's or portfolio's value or the individual's overall satisfaction or utility. Ideally, risk exposure should roughly be equal to risk tolerance. Risk management is **not** about minimizing risk, but about actively managing risks to achieve goals. The focus is on risk management (as opposed to return management) because it is possible to manage risk, but it is not always possible to manage returns.

3. The Risk Management Framework

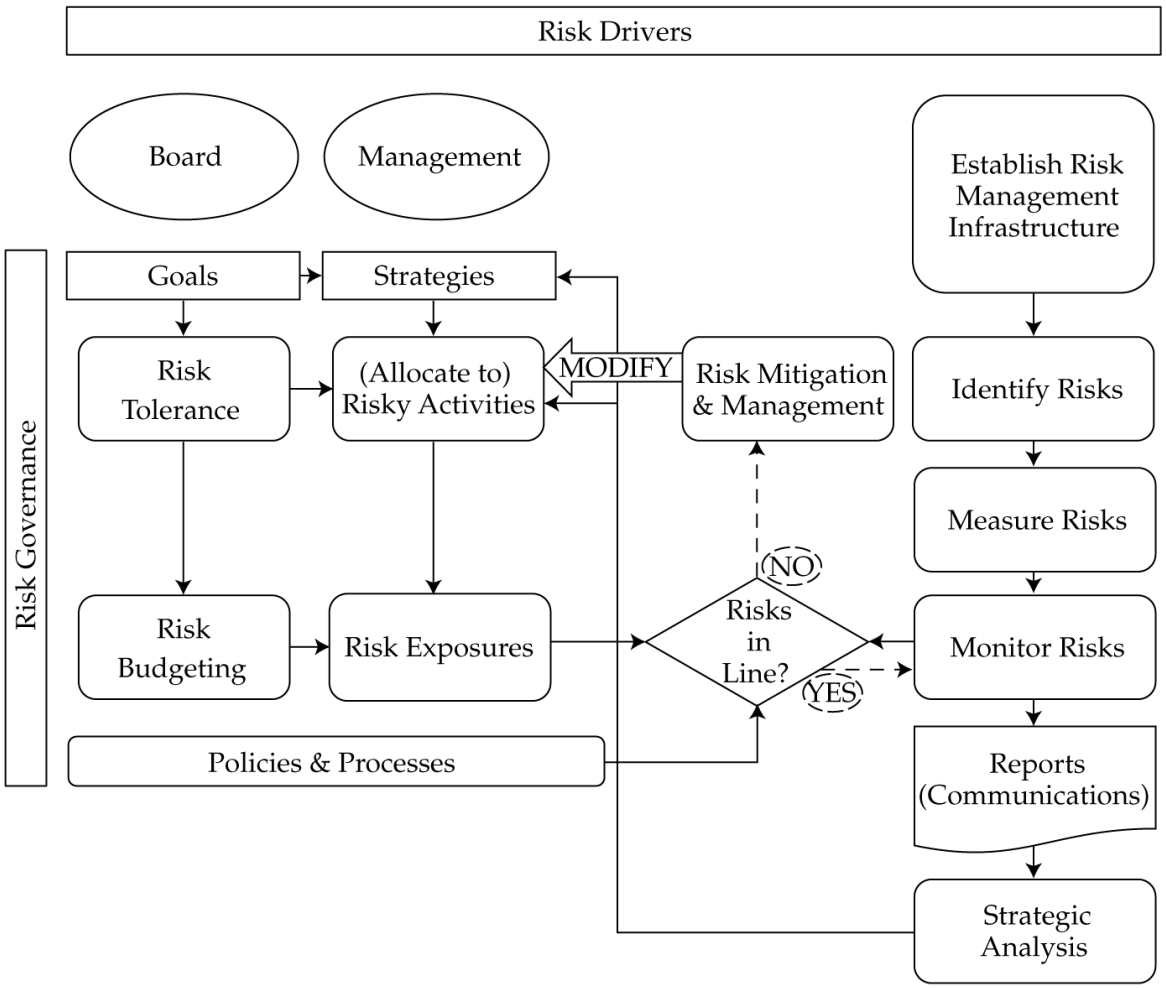
A risk management framework is the infrastructure, processes, and analytics needed to support effective risk management in an organization. Any risk management framework should include the following factors:

- Risk governance: This top-down process lays the foundation for risk management in an organization. Good governance ensures that the risk tolerance level is set for an organization and provides risk oversight.
- Risk identification and measurement: This is the quantitative and qualitative assessment of all sources of risk to an organization.
- Risk infrastructure: This refers to the people and the systems required to track risk exposures and to perform risk analysis.
- Defined policies and processes: These are limits, requirements, constraints, and

guidelines to ensure that an organization's risky activities are within its risk tolerance levels.

- Risk monitoring, mitigation, and management: This primarily involves identifying, measuring and continuously monitoring risk exposure of an organization. If risk exposure is not aligned with pre-defined risk tolerance, then necessary action is taken to restore balance between the two.
- Communications: Critical risk issues must be continually communicated across all levels of an organization. Risk tolerances must be communicated to managers. Risk metrics must be reported in a timely, easy-to-understand manner. A feedback loop with the governance body should be present to ensure that risk guidance is validated and communicated to the rest of the organization.
- Strategic analysis or integration: The objective of this analysis is to use risk management to increase the overall value of the business.

The diagram below shows the risk management framework in an enterprise context.



4. Risk Governance – An Enterprise View

4.1 An Enterprise View of Risk Governance

Risk governance is a top-down process that defines risk tolerance and provides guidance to align risk with enterprise goals. It includes guidance on unacceptable risks and worst losses that can be tolerated.

An enterprise risk management perspective deals with the whole organization. The governing body drives the risk framework in the following ways:

- It determines the goals of the organization.
- It is responsible for providing risk oversight to ensure that value is maximized.
- It determines the risk tolerance level; which risks are acceptable, which risks to mitigate, and which risks are unacceptable. The process includes guidance on worst losses that can be tolerated for every scenario.

Elements of good risk governance are as follows:

- To provide a forum where management can discuss the risk framework and key issues that come up during execution.
- Form a risk governance committee to oversee the implementation of the framework at an operational level relative to the high level oversight by the governance body.
- Appoint a chief risk officer (CRO) to build and implement the risk framework for the entire enterprise.

5. Risk Tolerance

Risk tolerance identifies the extent of losses an organization is willing to experience. Risk tolerance focuses on the appetite for risk of an organization in its pursuit of achieving goals and maximizing value. The process involves defining:

- Which risks are acceptable and which risks are not acceptable?
- How much risk can the entity be exposed to?

The risk tolerance decision begins with two different analyses:

- Inside view: What shortfalls within the organization will cause it to fail or not achieve certain goals?
- Outside view: What uncertain forces is the organization exposed to?

Using these two views in conjunction, the board will:

- Define which risks to take and which risks not to take.
- Determine the risk appetite: how much of these risks to take.
- Communicate risk tolerance before a crisis.
- Provide a high-level guidance to management in strategizing and choosing activities.

There are no standard formulas to determine the risk tolerance of a company. Some of the factors that will help a board determine its risk appetite are as follows:

- Company's areas of expertise and goals.
- Ability to respond dynamically to adverse events: The higher the ability, the higher the level of risk tolerance.
- The amount of loss a company can bear without impacting its status as a going concern.
- The company's position in the industry, and how it fares relative to its competitors.
- Government and regulatory landscape where the company operates.
- Quantitative analyses such as scenario analyses, macro analyses. etc.

Once risk tolerance is determined, the objective of the overall risk framework should be to align risk exposure with the enterprise's risk appetite.

6. Risk Budgeting

Risk budgeting helps determine how or where risks are taken and quantifies tolerable risks by specific metrics; risk budgeting should drive hedging strategies (not the other way round).

Risk budgeting allocates investments or assets by their risk characteristics rather than by a common classification of asset class such as stocks, bonds, real estate, etc. For example, the risk view of a portfolio might be that it is driven 70% by global equity returns, 20% by domestic equity returns, and 10% by interest rates, or a portfolio that has 45% illiquid and 55% liquid securities.

How risk budget is measured

- It can be a complex, multi-dimensional measure that evaluates risks based on their asset classes such as equity, commodities, and real estate and then allocates investment by their asset class.
- It can also be a simple, one-dimensional risk measure such as standard deviation, beta, and value at risk and scenario loss.
- Risk factor approaches are also used, in which exposure to various factors is used to determine risk premiums.
- Example: portfolio beta is limited to 1.

One of the biggest benefits of the risk budgeting process is that it forces a firm to consider risk trade-offs. By adopting risk budgeting, it helps a business to:

- Choose the project with the highest return per unit of risk.
- Choose between doing less risky investments and more risky investments whose risks have been hedged.
- Compare active versus passive strategies. This helps businesses make decisions to add active value while staying within the risk tolerance levels.

7. Identification of Risk – Financial and Non-Financial Risk

There are two categories of risks: financial risks and non-financial risks.

7.1 Financial Risks

Financial risks are the risks that originate from financial markets, such as changes in interest rates or prices. There are three primary types of financial risks:

- **Market risk**: This risk arises from movements in stock prices, exchange rates, interest rates, and commodity prices. Any changes in fundamental economic conditions, events in the industry or economy, give rise to market risk.
- **Credit risk**: This is the risk that a counterparty will not pay an amount owed on an obligation, such as a bond, loan, derivative, to another party.
- **Liquidity risk**: This is the risk that, as a result of degradation in market conditions or the lack of market participants, one will be unable to sell an asset without lowering the price to less than the fundamental value. Liquidity risk is also known as transaction cost risk. Liquidity risk arises when the market for a specific asset becomes less liquid or the size of a position increases.

7.2 Non-Financial Risks

Non-financial risks are risks that arise from sources outside the financial markets, "from actions within the organization or from external origins, such as the environment as well as from the relationship between the organization and counterparties, regulators, governments, suppliers, and customers".. These risks also have a monetary impact on the organization. The various types of non-financial risks are discussed below:

- **Operational risk**: This risk arises from within the operations of an organization and includes both human and system or process errors. All the internal risks in an organization are collectively called operational risk. Examples of operational risk include inadequate or failed employees, programming errors, systems, and internal policies, procedures and processes making an organization susceptible to hackers, rogue trader in a brokerage firm, natural disasters that interrupt operations, and terrorist attacks. Operational risk can also arise due to extreme weather and natural disasters such as floods, earthquakes, or hurricanes.
- **Solvency risk**: This risk arises when the entity does not survive or succeed because it runs out of cash to meet its financial obligations. One example of solvency risk is what happened to Lehman Brothers in 2008 because of taking on excessive leverage.
- **Settlement risk**: This is the default risk that occurs just before payments are to be settled.
- **Legal risk**: Any risk related to the law is a legal risk. For instance, an entity may be sued by another over a transaction, or what it does or does not do, as per the contract.
- **Regulatory, accounting, and tax risk**: The three risks are collectively known as compliance risk. This risk arises when an entity fails to comply with laws, regulations, and policies set by the government or regulatory authorities.
- **Model risk**: This is the risk of a valuation error that arises from improperly using a model. For instance, using the DDM (dividend discount model) to value a company

whose growth is not constant.

- **Tail risk**: This risk arises when there are more events in the tail of the distribution.
- **Sovereign or political risk**: This risk arises when political actions negatively impact a company.

Individuals face many of the same organizational risks outlined here, in addition they also face health risk, mortality or longevity risk, and property and casualty risk.

8. Identification of Risk – Interactions between Risks

Risks are not independent of each other and there is no clear distinction between the various risks as one risk may lead to another. For example, market risk leads to credit risk, which in turn leads to settlement risk and legal risk.

Risk interactions can be non-linear and harmful. The combined risk faced is worse than the sum of the risks of the separate components. This was seen during the 2008 crisis when many investment firms were forced to shut down because of their high leverage and insolvency. Most risk models do not take into account the interactions between risks.

9. Measuring and Modifying Risk – Drivers and Metrics

9.1 Drivers

Basic drivers of risk arise from:

- Global macroeconomics: The economic policies adopted by foreign governments and central banks have a significant impact on domestic companies.
- Domestic macroeconomics: Economic activity in a country is affected by the taxes, regulations, laws, monetary and fiscal policy introduced by government and quasi-government agencies in a country.
- Industries: Government's policies expose industries to risk. For example, the government may exempt taxes on the textile industry to encourage growth in the sector, while it may levy additional taxes on the tobacco industry.
- Individual companies: There could be an issue that is specific to the company that you have invested in. For example, a lawsuit.

Using proper risk management, some of the risk can be managed, but not all of it. For risks that cannot be controlled, an entity must ensure that its risk exposure is aligned with its objective and risk tolerance.

9.2 Metrics

Risk exposure is often expressed in terms of quantitative measures. The basic metrics used to measure market risk are as follows:

- **Probability**: It is a measure of the relative frequency with which an outcome is expected to occur. For instance, the probability of a loss of 25% implies the likelihood of incurring loss, but it does not say how much the loss would be.

- **Standard deviation**: It is a measure of the dispersion in a probability distribution. That is, it gives us a range over which a certain percentage of outcomes are likely to occur. The underlying assumption is that the returns are normally distributed. Hence, it is not an appropriate risk measure for non-normal distributions. Standard deviation and variance are measures of total risk, that is, both unsystematic and systematic risk.
- **Beta or duration**: It is a measure of the sensitivity of a security's returns to the returns on the market portfolio. For instance, if beta is 1.5, then it implies that the stock is expected to go up by 1.5% when the market goes up by 1%. Beta is generally used for stock portfolios, while duration is used to measure the sensitivity of fixed-income portfolios to changes in interest rates.
- **Derivative measures**: Delta, gamma, vega, and rho are often used measures of derivative risk. **Delta** is the sensitivity of the derivative price to a small change in the value of the underlying asset. **Gamma** measures the sensitivity of the derivative to changes in delta. **Vega** measures the sensitivity of the derivative to changes in the volatility of the underlying. **Rho** measures the sensitivity of the derivative to changes in interest rates.
- **Value at risk or VaR**: VaR measures and quantifies the risk of loss in a portfolio over a specific time period. A VaR measure comprises three elements: an amount stated in units of currency, a time period, and a probability. Let us take an example of a bank with a portfolio value of $200 million. A VaR of $3 million at 5% for one day implies that the bank is expected to lose a *minimum* of $3 million in one day 5% of the time. Note that VaR only tells us the minimum expected loss; it does not state the maximum loss.
- **Conditional VaR or CVaR**: Conditional VaR is the weighted average of all loss outcomes in the statistical distribution that exceed the VaR loss. It is a measure of expected loss.
- **Expected loss given default**: This is equivalent to CVaR for a debt security.
- **Scenario analysis and stress testing**: Stress test measure the impact of change in a specific variable such as interest rate or exchange rate. Scenario analysis measure the impact of a change in multiple variables simultaneously. Scenario analysts evaluate what would happen to a portfolio if a set of conditions or market movements occur. For example, what would be the impact on a portfolio if the Fed increases interest rates and there is a significant decline in the value of the US dollar?

10. Methods of Risk Modification – Prevention, Avoidance and Acceptance

The objective of the risk manager in the risk modification stage is to align the actual risk with pre-defined levels of risk tolerance. Different approaches to manage and modify risk are discussed below.

Risk Prevention and Avoidance

The simplest approach to manage risk may be to avoid it altogether. But, it is not as simple as it appears. For example, consider an individual who invests all his retirement savings in cash to avoid the risk of volatility in equities. By doing so, he gives up any upside return potential that equities offer and protection against inflation. Sometimes, boards may take a strategic decision to avoid risks in certain business areas altogether after analyzing the risk-return trade-off, and rather focus on areas with a higher likelihood of adding value. In reality, it is difficult to take a calculated risk by offsetting the risk of loss with the benefit of gain.

When actual risk exceeds the acceptable level, the following approaches are used to manage risk.

Risk Acceptance: Self-Insurance and Diversification

Self-insurance is simply bearing the risk because the external means to eliminate the risk are costly. For business, self-insurance means setting aside sufficient capital to cover losses. An example of self-insurance is capital and loan loss reserves set aside by a bank.

Diversification: According to modern portfolio theory, diversification is an efficient way of mitigating risk.

11. Methods of Risk Modification – Transfer, Shifting, Choosing a Method for Modifying

Next, we will look at two approaches to transfer or sell the undesired risk to another party.

Risk Transfer

Risk transfer is the process of passing on a risk to another party, often in the form of an insurance policy. When a corporation buys fire insurance for its office building it pays a standard premium and in return the insurance company covers the damage if the office building catches fire. Hence through the insurance policy the risk of fire damage is transferred from the corporation to the insurance company.

Risk Shifting

Unlike risk transfer where the risk is transferred from one party to another, risk shifting refers to actions that change the distribution of risk outcomes. Risk shifting typically involves the use of derivatives. Derivatives are classified into two categories:

- Forward commitments. Examples of forward commitments are forward contracts, futures contracts, and swaps.
- Contingent claims. Examples of contingent claims are call options and put options.

How to Choose Which Method for Modifying Risk

Choosing which risk mitigation method to use is an important step in the risk management process. The risk-mitigation methods discussed above are not exclusive of each other. Often,

companies use all methods. Some important points to consider how to choose a method are discussed below:

- Consider the cost and benefit of each option in light of the risk tolerance of the entity.
- Organizations should avoid the risks that provide few benefits at extremely high costs.
- Organizations with large free cash flow may self-insure and diversify to the extent possible.
- Insure when risks can be pooled effectively and when the cost of insurance is less than the expected benefit.
- Risk shifting is an appropriate choice for mitigating financial risks that exceed risk appetite.

Summary

LO.a: Define risk management.

Risk management is the process by which an organization or individual defines the level of risk to be taken (risk tolerance), measures the level of risk being taken (risk exposure), and modifies risk exposure in line with risk tolerance. The goal is to maximize the company's or portfolio's value or the individual's overall satisfaction or utility.

LO.b: Describe features of a risk management framework.

A risk management framework is the infrastructure, processes, and analytics needed to support effective risk management in an organization. The factors a risk management framework should include are risk governance; risk identification and measurement; risk infrastructure; risk policies and processes; risk monitoring, mitigation, and management; communication; and strategic analysis and integration.

LO.c: Define risk governance and describe elements of effective risk governance.

Risk governance is the top-level foundation for risk management. The governance body is responsible for setting risk tolerance and providing risk oversight.

The elements of effective risk governance include providing a forum where the management can discuss about the risk framework, the forming of a risk governance committee, and the appointing of a chief risk officer.

LO.d: Explain how risk tolerance affects risk management.

Risk tolerance identifies the extent of losses an organization is willing to experience. It defines which risks are acceptable, which risks are not acceptable, and how much risk an entity can be exposed to.

LO.e: Describe risk budgeting and its role in risk governance.

Risk budgeting quantifies tolerable risks by specific metrics. Risk budgeting allocates investments or assets by their risk characteristics rather than by a common classification of asset class such as stocks, bonds, real estate, etc.

LO.f: Identify financial and non-financial sources of risk and describe how they may interact.

Financial risks are the risks that originate from financial markets. Three types of financial risks include market risk, credit risk, and liquidity risk.

Non-financial risks are risks that arise from sources outside the financial markets. The various types of non-financial risks include operational risk, solvency risk, settlement risk, legal risk, regulatory risk, accounting and tax risk, model risk, tail risk, and sovereign or political risk.

Risks are not independent of each other and there is no clear distinction between the various

risks as one risk may lead to another.

LO.g: Describe methods for measuring and modifying risk exposures and factors to consider in choosing among the methods.

The four factors that drive risk are global and domestic macroeconomics, industries, and individual companies.

Common measures of market risk include probability, standard deviation, beta or duration, derivative measures, value at risk, conditional value at risk, expected loss given default, and scenario analysis and stress testing.

Risk can be modified by prevention, avoidance, risk transfer, or shifting.

When actual risk exceeds the acceptable level, risk can be mitigated through self-insurance and diversification.

The best method to choose to modify risk depends on the benefits weighed against the costs after considering the overall risk profile.

Practice Questions

1. Risk management process includes:
   A. maximizing returns.
   B. defining and measuring risks being taken.
   C. minimizing risk.

2. The correct sequence for risk management for an enterprise is:
   A. measuring risk exposures, establishing risk tolerance, and performing risk budgeting.
   B. establishing risk tolerance, measuring risk exposures, and performing risk budgeting.
   C. establishing risk tolerance, performing risk budgeting, and measuring risk exposures.

3. Which of the following factors of a risk management framework *most likely* addresses people and the systems required to track risk exposures?
   A. Governance.
   B. Communications.
   C. Risk infrastructure.

4. Risk governance is *best* described as:
   A. identification of individuals at each level of hierarchy for delegation of risk management responsibilities.
   B. aligning risk management with the goals of the entire organization.
   C. evaluation of potential sources of risk in an organization at each of its business unit.

5. Which of the following statements about risk tolerance is *most* accurate?
   A. The risk tolerance focuses on how any specific risk can be taken.
   B. Risk tolerance is best discussed ex ante, before awareness of risk is heightened.
   C. Risk tolerance defines the qualitative assessment and evaluation of potential sources of risk in an organization.

6. Which of the following is *most* consistent with a risk-budgeting approach to portfolio management?
   A. Risk budgeting quantifies tolerable risks by specific metrics.
   B. Risk budgeting involves defining the acceptable and non-acceptable level of risk.
   C. Risk budgeting involves allocating investments by their amount of underlying return sources or factors.

7. Which of the following is a financial risk?
   A. Model risk.
   B. Legal risk.
   C. Liquidity risk.

8. Which of the following is a non-financial risk?
   A. Operational risk.
   B. Credit risk.
   C. Market risk.

9. Which of the following is *least likely* an example of model risk?
   A. Assuming tails of a distribution of returns are thin without checking.
   B. Using the five-year risk-free rate to discount the face value of a five-year government bond
   C. Using standard deviation as a measure of risk in an asymmetric returns distribution.

10. Which of the following *best* describes an example of risk interaction?
    A. Exogenous shocks impact creditworthiness of a company thereby increasing credit risk to the company it owes money to. The increased credit risk increases the legal risk for the lender firm.
    B. Terrorist attacks in Europe cause a decline in US stock market.
    C. Political uncertainty in a region lowers economic prospects thereby raising the credit spreads.

11. Value at risk (VaR) of a firm is one-month 5% value at risk of $2 million. The *most appropriate* interpretation for this is:
    A. 95% of the time the firm is expected to lose at least $2 million in one-month.
    B. 5% of the time the firm is expected to lose at least $2 million in one-month.
    C. 5% of the time the firm is expected to lose at most $2 million in one-month.

12. Which of the following *best* describes a method of risk shifting?
    A. Buying insurance.
    B. Maintaining a reserve fund.
    C. Entering into a derivative contract.

13. Which of the following risk modification methods involves use of derivatives?
    A. Risk transfer
    B. Risk shifting
    C. Risk diversification

Solutions

1. B is correct. Risks need to be defined and measured so as to be consistent with the entity's chosen level of risk tolerance and target for returns or other outcomes.

2. C is correct. Risk tolerance defines the appetite for risk for an enterprise. Risk budgeting then determines how or where the risk is taken and quantifies risk on an enterprise level. Risk exposures can then be measured and compared with the acceptable risk.

3. C is correct. Risk infrastructure refers to the people and systems required to track risk exposures.
   - Risk governance: This top-down process lays the foundation for risk management in an organization. Good governance ensures that the risk tolerance level is set for an organization and provides risk oversight.
   - Communications: Critical risk issues must be continually communicated across all levels of an organization. Risk tolerances must be communicated to managers. Risk metrics must be reported in a timely, easy-to-understand manner. A feedback loop with the governance body should be present to ensure that risk guidance is validated and communicated to the rest of the organization.

4. B is correct. Risk governance is determined by a top-down approach. Firm-wide risk tolerance is determined, followed by providing risk oversight and guidance to align risk with enterprise goals. Risk tolerance identifies the risk taking ability of the entire organization. It is usually discussed ex-ante (before an adverse event).

5. B is correct. Risk tolerance best discussed before a crisis (ex ante). Risk tolerance and risk budgeting are different from each other because risk tolerance focuses on the appetite for risk and what is and is not acceptable, risk budgeting has a more specific focus on how that risk is taken.

6. A is correct. Risk budgeting helps determine how or where risks are taken and quantifies tolerable risks by specific metrics. B is incorrect because risk tolerance involves defining the acceptable and non-acceptable level of risk. C is incorrect because risk budgeting allocates investments or assets by their amount of underlying risk sources not return sources.

7. C is correct. Financial risk originates form the financial markets. Credit risk, market risk, and liquidity risk are financial risks.

8. A is correct. Non-financial risk can originate from within the organization or from external sources like the society, environment, regulators, vendors, and customers. It

includes regulatory risk, government or political risk, solvency risk, operational risk, legal risk, accounting risk, model risk, and tail risk.

9. B is correct. Assuming tails of a distribution are thin and assuming symmetry of returns in asymmetric returns distribution are examples of model risk. Using the risk-free rate to discount the government bond is usually appropriate.

10. A is correct. In situation A, a market risk impacts all the firms. But the decline in the creditworthiness exposes other parties to credit risk and legal risk. This is an interaction among risks. Situations B and C represent single events of risk.

11. B is correct. VaR measures a minimum loss expected over a holding period a certain percentage of the time.

12. C is correct. Maintaining a reserve fund is a method of risk acceptance (self-insurance). Buying insurance is a method of risk transfer and using derivatives is a method of risk-shifting.

13. B is correct. Risk shifting refers to actions that change the distribution of risk outcomes. Risk shifting typically involves the use of derivatives. Risk transfer is the process of passing on a risk to another party, often in the form of an insurance policy. There is no method as risk diversification. Diversification is a part of Risk Acceptance method.

