2017 Edition

CIA

Preparatory Program

Part 3

Sample

Risk Management

Brian Hock, CIA, CMA
and
Carl Burch, CIA, CMA

Hock international

HOCK *international*, LLC
P.O. Box 6553
Columbus, Ohio 43206

(866) 807-HOCK or (866) 807-4625
(281) 652-5768

www.hockinternational.com
cia@hockinternational.com

Published January 2017

Acknowledgements

Acknowledgement is due to the Institute of Internal Auditors for permission to use copyrighted questions and problems from the Certified Internal Auditor Examinations by The Institute of Internal Auditors, Inc., 247 Maitland Avenue, Altamonte Springs, Florida 32701 USA. Reprinted with permission.

The authors would also like to thank the Institute of Certified Management Accountants for permission to use questions and problems from past CMA Exams. The questions and unofficial answers are copyrighted by the Certified Institute of Management Accountants and have been used here with their permission.

The authors also wish to thank the IT Governance Institute for permission to make use of concepts from the publication Control Objectives for Information and related Technology (COBIT) 3rd Edition, © 2000, IT Governance Institute, www.itgi.org. Reproduction without permission is not permitted.

Thanks

The authors would like to thank the following people for their assistance in the production of this material:

- Lynn Roden, CMA for her assistance in the technical elements of the material,
- Kevin Hock for his work in the formatting and layout of the material,
- All of the staff of HOCK Training and HOCK *international* for their patience in the multiple revisions of the material,
- The students of HOCK Training in all of our classrooms and the students of HOCK *international* in our Distance Learning Program who have made suggestions, comments and recommendations for the material,
- Most importantly, to our families and spouses, for their patience in the long hours and travel that have gone into these materials.

Editorial Notes

Throughout these materials, we have chosen particular language, spellings, structures and grammar in order to be consistent and comprehensible for all readers. HOCK study materials are used by candidates from countries throughout the world, and for many, English is a second language. We are aware that our choices may not always adhere to "formal" standards, but our efforts are focused on making the study process easy for all of our candidates. Nonetheless, we continue to welcome your meaningful corrections and ideas for creating better materials.

This material is designed exclusively to assist people in their exam preparation. No information in the material should be construed as authoritative business, accounting or consulting advice. Appropriate professionals should be consulted for such advice and consulting.

Section II – Risk Management

This section covers 10–20% of the exam and it is tested at a **proficiency level**. The two primary topics covered in this section are **risk management techniques** and **organizational use of risk frameworks**.

Note: The topic of risk management has gained importance in the past couple of decades as a result of individual company failings and larger market-wide failings in the economy. To some extent, recent corporate failings were the result of improperly managed risk. As a result, organizations took on more risk than they reasonably should have, and when the financial markets moved unfavorably the value of their assets plummeted.

Risk Management Techniques

This section begins by discussing risk and the benefits of risk management. In order for an organization to develop a risk management process, it first needs to understand its **risk appetite**, which is the amount of risk the company is able and willing to take on. Once a company establishes its risk appetite, it can implement an appropriate, tailor-made risk management process. This section covers the factors that influence an organization's risk appetite.

Organizational Use of Risk Frameworks

The section covers the methods through which organizations can manage their **financial** and **operational** risks. The discussion focuses on Enterprise Risk Management (ERM), in which a company embraces risk assessment throughout the organization and looks at the organization as a whole in making risk assessments.

This section makes up 10–20% of the exam, so it is an important topic to study thoroughly. However, as with Section I, many questions can be answered through common sense and from your own experience as an internal auditor.

IIA. Risk Management Techniques

The IIA defines risk management as "a process to identify, assess, manage and control potential events or situations, and provide reasonable assurance regarding the achievement of the organization's objectives."[6]

The following are two important ideas related to risk management:

- **Risk** is the probability that a future event or action could adversely impact the organization. Risk is measured in terms of the financial impact (in dollars) and the likelihood (or probability) of an event occurring.
- **Risk Assessment** is the process of analyzing and integrating professional judgments about probable adverse conditions and events in order to develop the audit work-schedule. The CAE should generally assign higher audit priorities to high-risk activities.[7]

  Risk assessment can be summarized in this manner:

  > Every entity faces a variety of risks from external and internal sources that must be assessed. A pre-condition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk Assessment is the identification and analysis of relevant risks to achievement of objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.[8]

[6] IIA's *Standards* Glossary, pg. 21.
[7] SIAS *No. 9 – Risk Assessment* 520.04.10.
[8] COSO, *Internal Control-Integrated Framework*, Executive Summary, pg. 3.

Benefits of Risk Management

Every organization needs to engage in risk management. Through proper risk management, an organization can reduce the probability of negative events occurring; in addition, with appropriate risk management the organization can reduce any negative impacts should a negative event occur.

The benefits from a risk management process depend, to some extent, on the industry the organization operates in; however, organizations can derive the following benefits as a result of prudent risk management:

- Increased shareholder value, (because risk management minimizes losses and maximizes opportunities)
- Fewer disruptions, shocks, and unwelcomed surprises to the operations of the business
- Employees, stakeholders, and governing and regulatory bodies have increased confidence in the organization
- More effective strategic planning
- Better cost control
- Quick assessment and grasp of new opportunities
- More complete contingency planning
- Improved ability to meet objectives and achieve opportunities
- Quicker response to opportunities

Risk Appetite

Risk appetite reflects the level of risk a company can optimally handle, given its capabilities and the expectation of its various stakeholders, such as vendors and creditors. Various industry groups have their own specific definitions of risk appetite, shown in the following chart:

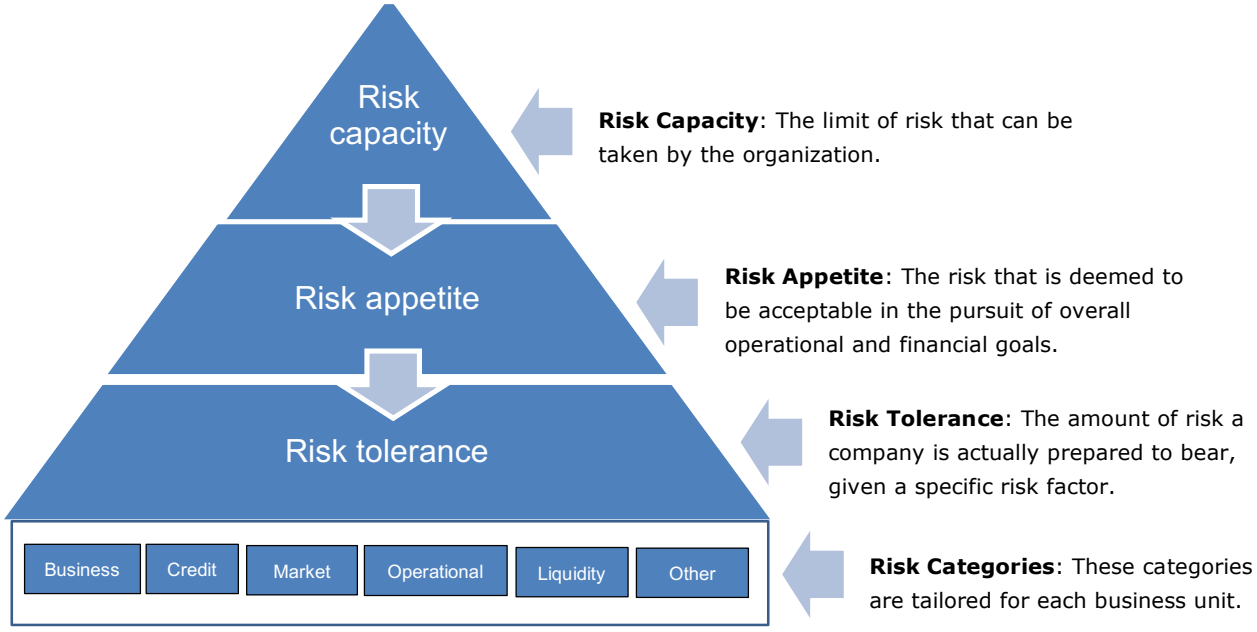
Organization	Definition
COSO's ERM framework	"The amount of risk an entity is willing to accept in pursuit of value."
The Institute of Internal Auditors (January 2009)	"The level of risk that an organization is willing to accept."
ISO 31000:2009/ISO Guide 73:2009	"Amount of risk that an organization is will to pursue or retain or take." (ISO 31000: 2009 does not use the word "risk appetite" but instead focuses on "**risk attitude**" and "**risk criteria**.")
Society of Actuaries ERM Symposium (April 2010)	"The level of risk that company management deems to be acceptable in pursuit of overall financial and solvency goals."
HM Treasury's Orange Book	"The amount of risk which is judged to be tolerable and justifiable."

Management must consider and balance the many different **views** and **risk factors**, with the final decisions being made at the corporate level (that is, using a **top-down approach**). In a sense, a company's risk appetite can reveal a great deal about its corporate culture. Balancing risk appetite and control is not easy, but it is a process that companies need to perfect if they are to succeed. For example, if a financial institution is actively involved with complex financial instruments (such as forward contracts, futures, options, or swaps), all relevant stakeholders need to know whether or not the company's directors understand the function of these instruments and the reasons for which the company is involved with them. Understanding a company's risk appetite is useful for ascertaining the **goal congruence** between the wishes of the board and the actions of management.

Risk Appetite, Capacity, and Tolerance

Two additional terms are useful for understanding risk appetite: **risk capacity** and **risk tolerance**. The figure below illustrates and defines the interrelatedness of risk capacity and risk tolerance.

Risk Capacity, Appetite, and Tolerance

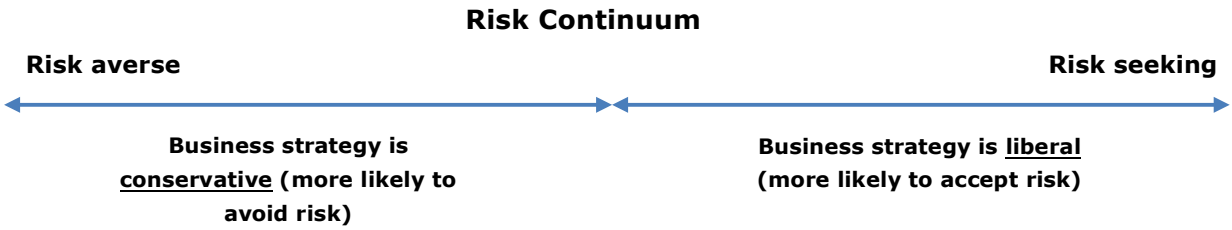


As this diagram indicates, a company must first determine its **risk capacity** in order to decide its **risk appetite**. Risk capacity is the absolute limit a company is willing to lose without bankrupting itself. Once a company gauges its risk capacity, it can ascertain how much it is willing and able to lose—that is, its risk appetite. Therefore, **risk appetite must be set within the limits of risk capacity.** Once risk capacity and appetite are established, **risk tolerance** represents the actual level of risk a company is able to bear, which can be determined through a combination of certain specific risk factors, shown as **risk categories** in the diagram. For example, if a company extends credit to its customers, then the company exposes itself to **credit risk** (that is, the risk that the customer will default). Given such possibilities, the company has to be completely clear about the amount of debt it can tolerate.

Different Attitudes Towards Risk

Businesses must assume risks in order to grow and survive. A **risk-averse** business is not necessarily trying to avoid risk; rather, it is seeking to obtain a reasonable, safe return for the comparatively low risk it is willing to undertake. On the other hand, **risk-seeking** businesses focus on maximizing their returns, and thus they may be less concerned about the level of risk that they assume.

The range of attitudes that businesses have towards risk can be shown in the **Risk Continuum** diagram (shown below). The left-hand side indicates businesses that are averse to taking on risk and whose strategies are therefore designed to avoid risk. On the right-hand side are businesses that actively seek out and accept risks. The ends of the diagram represent two extreme conditions, and most companies situate their place on the continuum somewhere in between these polar opposites.



No matter where a business situates itself on this continuum, it should be concerned about reducing risk without completely eliminating it. The function of risk appetite in this regard is to show the business where it is on this continuum: either risk averse or risk seeking. It is important to consider risk appetite when business strategies are being formulated and developed[9]; in fact, **business strategy** and **risk appetite** are so intertwined that both must be considered together.

Example: To illustrate the factors relevant to adopting a high-risk-seeking strategy, consider the example of a defense contractor dealing in computer software protection. This contractor decides to direct all corporate resources to a single product: a new software program to protect highly classified defense information from viruses and hackers. Through appropriate due diligence, it is determined that a successful bid will result in an extremely profitable windfall for the company. However, the tremendous investment of time and resources means that failure to secure the government contract will unavoidably result in bankruptcy. Clearly, this strategy represents a high level of risk appetite. Therefore, before moving forward on this decision, the board must consider all pertinent angles and sign off on the plan, thus indicating their acknowledgement and acceptance of the risk-seeking strategy. It is also possible that investors may approve this approach by increasing the value of the company's stock; conversely, they may punish the company by selling off shares. Either way, the direction of investor activity greatly depends on their own assessment of the company's position on the risk continuum.

Influences on a Company's Risk Appetite

The following is a list of the many factors that can influence a company's risk appetite:

- **The company's position in the business-development life cycle**. A company in the **start-up** phase will often require a high risk-appetite; indeed, 50% of US companies fail within their first five years. If a company survives the start-up phase and moves into the **growth stage**, it will need tighter controls to manage risk. Companies in this stage might establish an internal control function to oversee control and risk processes. Once companies enter the **maturity stage**, sales generally level off, which means that the focus switches to controlling cost, which can be done by taking advantage of increased productivity gains (perhaps through expanding overseas or developing other products).
- **The viewpoints of the major stakeholders**, including the company's major shareholders, bondholders, lenders, analysts, and many others. Each one of these stakeholders might have a different opinion as to how much risk the company should be willing to take on. For example, shareholders looking for higher returns might press a company to take greater risks; however, the bank that lent the company money might prefer limits on risk-taking.

[9] COSO, *Enterprise Risk Management – Integrated Framework*, Understanding and Communicating Risk Appetite, pg. 4.

Example: Whether or not a particular viewpoint is taken into account will depend on how much influence or power a given stakeholder has. For example, if a bank lends a company a substantial amount of money, then the bank will have a strong interest in the company's continued existence. If the bank feels that the company is taking unnecessary risks, then it could be in a position to voice its concerns to management and to the board. The level of concern the bank expresses would be directly proportional to the amount it has invested (that is, more investment, more level of concern). In addition, the likelihood that the bank's concerns will influence company policy also rises in proportion to its level of investment (that is, more investment means more influence).

- **Accounting factors**, such as the volume of transactions, the complexity of the accounting system, changing rules and regulations, and so forth.
- The **opportunity for fraud** to be committed.
- **External factors**, such as changing economic considerations, changes in the industry, changes in technology, and so forth. For example, if an economy in which a company operates is going through a recession, the company may decide that a larger bad-debt provision would be appropriate to take into account the possibility of more consumer bad debt. If an industry comes under more scrutiny because of environmental issues, the company might also decide that it needs a provision for environmental contamination.
- **Governmental restrictions**. Depending on the industry, governments can dictate the level of risk a company is able to take on. Industries such as insurance and banking are generally more regulated and more restricted than other companies because they are responsible for the public's money.
- **Entity-level factors**, such as the quantity and quality of hired personnel, quantity and quality of training courses, disruptions in the information system processing system, changes in the organization's structure, and changes in key personnel.

Risk-taking and Cultural Considerations

Companies that operate across national and cultural borders will encounter a range of practices and expectations. In setting business strategies, a company might choose to adopt what appears to be the path of least resistance, which is to export the corporate and management philosophies of the "home" country to the cross-border or overseas divisions. However, cultural insensitivity may cause unintentional but serious harm to relationships with employees and customers and damage a company's potential for success.

Risk-taking, particularly in the business environment, is a subject that is closely connected to cultural practices and beliefs, and therefore management should carefully study and understand the regional attitudes about risk-taking before implementing a particular set of objectives and the methods for achieving them. By gaining an understanding of risk-taking attitudes in the overseas culture, a company has much to gain. Foremost, a company can cultivate strong ties with employees and business associates. Second, potential pitfalls (such as unintentional offense or misunderstandings) can be avoided. Third, a culture-sensitive company can derive an advantage over their less-aware competitors by demonstrating a willingness to take the local culture into account.

That said, it is not necessary for a company to remove all ties to the "home" culture, since doing so might very well jeopardize the identity that makes a company distinct among its competitors—and risk-taking strategies are certainly an important component of a company's identity. Striking the right balance between the organization's "home" culture and other nations' culture is a delicate but rewarding process. Toward this goal, **cross-cultural training** (such as through consultants or retreats) is an effective means of creating inter-cultural dialogue, communicating company goals, and addressing and bridging cultural differences.

Formalizing Risk Appetite

If a company has not made a **formal statement** about its risk appetite, then it has a potential control problem. Without such a statement, managers could be running the company with insufficient guidance on the levels of risk that they are permitted to take, or they may not be seizing important opportunities due to a perception that taking on additional risk is discouraged.

Formalizing risk appetite means putting it in writing so that there is little confusion about the board and management's attitude toward risk. Indeed, formalizing risk appetite improves communication between all those who oversee risk management. Generally speaking, the larger and more complex an organization is, the more formalized its policies and procedures should be regarding risk appetite. For example, large financial services companies (such as Citibank, Bank of America, BNP Paribas, ING, HSBC and others) can be expected to have highly detailed risk-appetite statements, whereas a small or mid-sized company might have a risk-appetite statement no more than a sentence or two.

Example: a short risk-appetite statement may be "no project investment should be greater than 20% of company's net assets" or "IFRS earnings should not be negatively affected by more than 50% of its forecasted earnings."

Risk appetite can be expressed either **quantitatively (numerically)** or **qualitatively**. The following are examples of quantitatively expressing risk appetite:

- **Solvency.** A company does not want to lose more than a defined amount of its capital so that it can remain a going concern following an extreme-loss event or combination of extreme-loss events.
- **Capital coverage.** A company requires that its capital is sufficient to cover a multiple of the amount of capital needed to absorb a loss of a certain magnitude (for example, a 1-in-100-year event).
- **Earnings.** A company does not want to lose more than a defined percent or multiple of annual net income.
- **Company value.** A company wants to assume the amount and kinds of risks that maximizes company value (that is, the risk adjusted present value of future cash flows).

There may be aspects of risk that cannot be measured quantitatively but regardless of the measurement limitations, risk still has to be identified. In such cases, "risk preferences" can be used to determine and establish risk appetite. **Risk preferences** define certain risk that the company does not want to accept, such as avoiding investment in subprime mortgages or taking out variable-annuity loans.

Once a company understands its risk appetite, it can start developing its risk management process.

Types of Risk

The following is a list of four common categories of risks:

1) **Strategic risks** occur on a global or macro level, such as unexpected fluctuations in the global economy or related market conditions, political risk, and risks that are connected to the company itself, such as reputation risk, brand risk (patent and trademark protection), leadership risk, or the risk of customers' needs changing. Strategic risks can be related to actions of competitors and changes in the regulations businesses are subject to, as regulatory changes could cause significant increases in compliance expense. Capital availability is another strategic risk.

   The company will need to identify strategic risks, be aware of them, and monitor them. However, it is unlikely that the company can actively influence the global economy or the political environment in which it operates.

2) **Operational risks** result from inadequate or failed internal processes, people, or systems. Examples of operational risks include technology, business continuity, customer satisfaction, and the risk of

product or service failure. Because operational risks are more directly under the influence of management, the company is in a better position to mitigate these issues through its own actions.

Operational risk also includes legal and compliance risks. **Legal risks** are associated with uncertainty due to litigation or uncertainty in the applicability or interpretation of contracts, laws, or regulations. **Compliance risk** refers to the danger that current or future profits or assets may be negatively impacted as a result of violations of, or nonconformance with, laws, rules, regulations, required practices, internal policies and procedures, or ethical standards.

3) **Financial risks** are connected to the financial health of the company. Examples include volatility of foreign currencies, volatility of interest rates, volatility of commodity prices (inputs), credit risk, liquidity risk, and market risk.

   When a company borrows money from a lending institution, it engages in two forms of financial risk:

   a. **The risk that the company will not be able to pay its interest and other obligations.** As the firm increases the proportion of debt financing to total financing in its capital structure, its fixed cash outflows for interest expense will increase. As a firm's cash outflows for interest expense increase, the possibility of the firm's becoming insolvent increases.

   b. **The presence of debt and interest payments increases variability in earnings per share.** Borrowing affects the fixed interest costs on the firm's net income, and fixed interest costs increase the volatility of a firm's Earnings Before Taxes (EBT).

4) **Hazard risk** refers to harmful or catastrophic events that can be insured against. Examples of hazard risks and their relevant remedies (in parentheses) include natural disasters (property insurance), death of a key employee (key-person life insurance), and personal injury that takes place on the premises of the business (liability insurance).

Volatility affects the consistency of expected results and increases risk because it introduces uncertainty about the future. Greater volatility means that there is a higher probability that future results will be poor.

The **time period** under consideration is also a crucial factor in risk. Risk increases in proportion to the length of time because with more time there are more chances for something to go wrong.

Note: Volatility and time period are not completely negative factors. There is always a chance that volatility and a lengthy time period might yield better than usual or better results. However, this section on risk will concentrate primarily on the negative aspects.

Political risk, a form of strategic risk, is the likelihood that a political event will cause an investment's value to change or become worthless. Political risks include government **expropriation** (seizure of private property with minimal or no compensation), **war**, **blockage of fund transfers**, **inconvertible currency** (that is, a government prevent its currency from being exchanged for other currencies); **bureaucracy**, **regulations**, **taxes**, **corruption**, and even **consumer bias** (preferring local rather than foreign products).

Internal and External Risk

Risks can be classified as internal or external.

Examples of internal risks:

- **Infrastructure events**, such as organizational or policy changes, which can cause a rise in customer complaints and a decrease in customer satisfaction. Expansion of facilities carries a risk that the increased production will not be accepted in the marketplace.
- **Process-related events**, such as changes in the way an item is produced. Changes in processes can cause a range of risk events, like processing errors and omissions.
- **Internal technological events**, such as new software that may not work properly, improper setup, and inadequate user training.

Examples of external risks:

- **Competition** and actions of competitors.
- **Regulations** and compliance problems.
- **Supply chain disruptions**.
- **Political risk**.

Question 1: The lawyers of Regional Tobacco Company have recently informed management that they believe that the company may lose an ongoing court case and as a result will be forced to pay a large monetary damage. The characteristics of the court and judicial system that influence the frequency and severity of losses is known as

a) Moral hazard.

b) Compliance risk.

c) Speculative risk.

d) Legal risk.

(HOCK)

Question 2: Mike Smith is the CFO at TechEquip Inc., a manufacturer of computer equipment. Smith learned last week that the accounting department has not completed any bank reconciliations for the last six months due to the implementation of a new accounting software package. What type of risk has Smith identified?

a) Financial risk

b) Hazard risk

c) Operational risk

d) Strategic risk

(ICMA)

Question 3: Riverfront Properties' new apartment building was almost complete. There were a few inspections left to pass, and they did not have a certificate of occupancy. However, the owner felt that they were close enough that he allowed new tenants to begin moving in. The risk that the owner has created in this situation is best described as

a) Operational risk, because the owner was not in compliance with laws and regulations.

b) Strategic risk, because the owner was not in compliance with laws and regulations.

c) Strategic risk, because the remaining inspections could determine that the building is uninhabitable.

d) Operational risk, because the remaining inspections could determine that the building is uninhabitable.

(ICMA)

The Risk Management Process

Below is a general approach to the risk management process. When applying these guidelines to a company, department, or specific situation, steps may be added or altered to take into account the specific situation and the state of the company's existing risk management process.

The steps are:

1) Risk identification
2) Risk assessment.
3) Risk prioritization
4) Response planning
5) Risk monitoring

Step 1: Risk Identification

To begin, management must identify risks that have some probability of occurring and impacting operations. Risk identification needs to be balanced with the company's strategic goals. At the same time, management must take into consideration the threats and opportunities the business faces along with the strengths and weaknesses within the business itself.

Outside the rare exception of a catastrophic event, it is unusual for a single event or risk factor to affect the entire company at once. Even so, the risk-identification process should be conducted at all levels of the organization, since certain risk events may affect only one or a few segments of the company. An effective risk-identification strategy identifies key people within each unit (such as operations, finance and accounting, IT, and management) to take part in the identification and assessment of risks in their areas of responsibility.

Step 2: Risk Assessment

Next, identified risks are quantified, being evaluated for their **likelihood of occurring** and **relative significance**. The amount of potential financial loss is estimated along with other nonfinancial considerations.

Exposure to risk is assessed according to the **loss frequency or probability** and the **loss severity**.

1) **Loss frequency** or **probability** measures how often the loss occurs on average, and it is expressed in relation to a time period. A loss frequency of "0.25 per year" means that the probability is 25% that a loss will take place in any given year, and therefore on average a loss occurs once every four years.
2) **Loss severity** measures the financial impact of a loss. For example, a company may determine that historically when a particular loss has occurred, the average cost of the loss to the company has been $50,000.

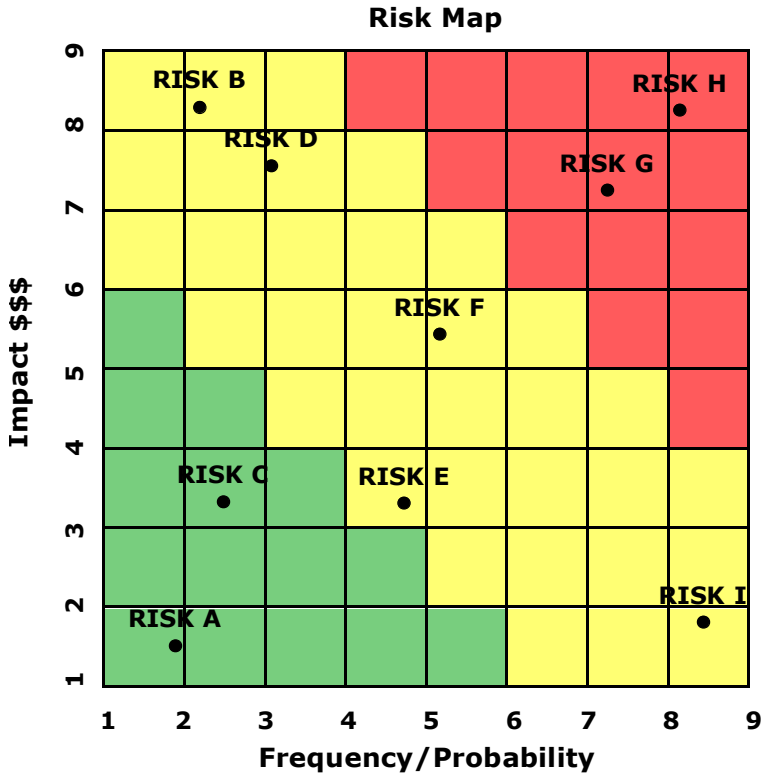
Qualitative Risk Assessment Tools

To make the risk assessment process efficient, identified risks need to be prioritized so that management knows which issues require the most immediate attention. Although financial risks are key considerations, the company should also consider qualitative factors, such as the potential for lost customer goodwill. Therefore, to a large extent **risk ranking** is a qualitative assessment.

Qualitative assessment can be visualized by means of a **risk map** or **risk heat map**. For each identified risk, the **probability of the event happening** is plotted on the x-axis on a scale of 1 to 9; in addition, the **estimated impact of the loss** is plotted on the y-axis, also on a scale of 1 to 9. A risk map helps identify risks that are both more likely to occur and that have a greater potential for loss. If a particular risk involves quantitative factors such as financial loss, the potential quantitative loss is included in the assessment.

Qualitative risk assessment can also be done without calculating the amount of loss as a specific amount. It can rank the amount at risk from the highest to the lowest for the different risk events.

The following chart shows a combination of assessed risks, mapped according to probable frequency (red is the most frequent, green the least frequent) and the amount of financial impact (in US dollars):



In this risk map, Risks A and C have low financial impact and low probability; therefore, they should be assigned low priority. Conversely, Risks G and H have high financial impact and high probability; therefore, they should be placed high on the priority list.

This kind of qualitative risk assessment can identify serious risks that may not have an immediate or obvious financial impact but which still could prove damaging to the company. Consider Risk I. Its financial impact is not as great as Risks B and D and therefore it might rank low on the priority list. However, Risk I has a very high probability rating, meaning that it is much more likely to happen than Risks B and D. As a result, management should seriously consider moving Risk I up the priority chain.

Quantitative Risk Assessment Tools

The following is a list of quantitative assessment tools:

- **Value at Risk (VaR)** measures the potential loss in value of a risky asset or event over a defined period for a given confidence interval. VaR is based on the assumption that the possible outcome of the event is represented by a normal distribution. With a normal distribution, 95% of the results will lie within 1.96 standard deviations of the mean and 99% of the results will lie within 2.57 standard deviations of the mean. This information can help predict the range of results with a measured level of confidence.

  Example: If the VaR on an asset is $100 million at a one-week, 95% confidence level, there is only a 5% chance that its value will drop more than $100 million over any given week.

- **Cash Flow at Risk** measures the likelihood that cash flows will drop by more than a certain amount. Cash Flow at Risk also uses the measures of a normal distribution.

- **Earnings at Risk** measures the confidence interval for a fall in earnings during a specific period.
- **Earnings Distributions** is a graphical representation of the probability of a level of return and the level of return itself.
- **Earnings per Share Distributions** is a graphical representation of the probability of the amount of earnings per share (EPS) and the likelihood of each level occurring.
- **Benchmarking** compares the organization's risk profile and the impact of the risks it faces against those of similar companies.

In addition, other quantitative techniques can be used to assess risks. Breakeven analysis, sensitivity analysis, decision trees, simulation analysis, and scenario analysis can help to determine which risks have the most potential impact on a project.

Question 4: The measure that provides a quantitative measure of the accuracy of the potential financial loss is

a) Residual risk.

b) Inherent risk.

c) Risk ranking.

d) Value at risk.

(HOCK)

Step 3: Risk Prioritization (Ranking)

After risks have been identified and assessed, the company must decide which risks should receive the highest priority. This decision includes quantitative and qualitative analysis.

The following four terms measure the potential loss associated with identified risks:

1) Expected Loss (given a set of probabilities)
2) Unexpected Loss
3) Maximum Probable Loss
4) Maximum Possible Loss (also called Extreme or Catastrophic Loss)

1) Expected Loss

An expected loss is the amount that management expects to lose to a given risk per year **on average** over a period of several years. **Because the loss is expected, it should be included in the budget**. Expected loss can be calculated in different ways depending on the specific situation that is being assessed.

First, for a specific event that has multiple probable outcomes, expected loss can be calculated as the weighted average of all the possible losses, using the probabilities of each of those losses coming to pass as the weights. Over the long term, the expected loss is the **average** amount of loss the company expects to incur during any given period.

Example: Assume that a company has determined that an event has the following probabilities of loss from a particular risk during a one-year period:

Probability	Amount of Loss
10%	$100,000
20%	$120,000
30%	$160,000
35%	$180,000
5%	$500,000

The probabilities must add up to 100%. The expected loss is calculated by multiplying each possible result by the probability (percentage chance) it has of occurring and adding these results together, as follows:

10%	×	$100,000	=	$10,000
20%	×	$120,000	=	$24,000
30%	×	$160,000	=	$48,000
35%	×	$180,000	=	$63,000
5%	×	$500,000	=	$25,000
				$170,000

Even though $170,000 is not one of the possible outcomes, it is the expected loss, a weighted average of all the possible losses given their probabilities.

Obviously, this process is greatly influenced by the possible outcomes and probability that is assigned to each outcome. For example, if the $500,000 loss had been given a higher than 5% chance of occurring, the expected loss would have been higher.

Second, expected loss can also be calculated for events that may or may not happen. For example, it is possible that there is a 40% chance an event will occur and a 60% chance that it will not occur. When loss is quantified in this way, there is only one probability for each risk: its probability of occurring.

The expected loss from each event is calculated by multiplying the dollar amount of each potential loss by the probability the event will occur. The amount of loss that results for each risk balances the amount of the loss with the probability of loss. The resulting loss amounts enable companies to better identify which risks are most important.

Example: A company has identified four risks. Below is the probability of occurrence for each risk during a one-year period and the amount of each loss if the risk does occur.

	Probability	Amount of Loss
Risk A	10%	$1,000,000
Risk B	25%	$600,000
Risk C	40%	$400,000
Risk D	90%	$200,000

Notice that these probabilities **do not sum to 100%**. They should not sum to 100% because each one represents the probability that a different event will occur. Each risk probability is independent of all the others.

A $100,000 expected loss for Risk A does **not** mean the annual loss from Risk A will be $100,000. It means that in 9 out of 10 years Risk A will not occur. In 1 out of 10 years, however, Risk A will occur and the loss will be $1,000,000. By extension, when that one-time $1,000,000 loss is averaged over a period of 10 years, the average expected loss **per year** is $100,000 ($1,000,000 ÷ 10).

Using the shortcut method, the expected value of each loss is calculated by multiplying the amount of the loss by the probability of its occurrence, as follows:

Risk A	10%	×	$1,000,000	=	$100,000
Risk B	25%	×	$600,000	=	$150,000
Risk C	40%	×	$400,000	=	$160,000
Risk D	90%	×	$200,000	=	$180,000

The expected value of each loss can be used to determine the most critical potential loss event. In this example, the risk item that has the lowest dollar amount of loss ($200,000) is probably the most critical to the company because of the high likelihood that it will occur. Its high probability of occurring causes its expected loss ($180,000) to be the highest of the four identified risks.

The following risks are ranked according to their expected values:

#1	Risk D	90%	×	$200,000	=	$180,000
#2	Risk C	40%	×	$400,000	=	$160,000
#3	Risk B	25%	×	$600,000	=	$150,000
#4	Risk A	10%	×	$1,000,000	=	$100,000

2) Unexpected Loss

An unexpected loss is the amount that **could likely** be lost to a risk in a very bad year, **in excess of the amount budgeted for the expected loss**, up to the maximum probable loss. The business should reserve the unexpected loss amount as capital.

3) Maximum Probable Loss

The maximum probable loss (also called the probable maximum loss [PML]) is **the largest loss that can occur under foreseeable circumstances**. The maximum probable loss is the largest amount of damage that **could likely** occur in a very bad year. Damage greater than the maximum probable loss **could** occur, but such an outcome is very unlikely.

If the risk is to real property, the estimated maximum probable loss would take into consideration the property's characteristics. The maximum probable loss to real property is inversely related to the size of the building and to the effectiveness of protection in place. For example, the larger the building is, the less probability there is that the entire structure would be destroyed. The better the fire suppression is, the more likely it is that a fire would be brought under control and extinguished completely before the whole building is destroyed. The building's state of occupancy also influences the amount of damage that could occur. A vacant building is more vulnerable to vandalism or destruction than an occupied building since occupants are in a position to intervene.

4) Maximum Possible or Catastrophic Loss

Maximum possible or catastrophic loss is the worst-case scenario, the greatest possible loss from a specific risk or event. For example, if the risk is loss of property, the maximum possible loss is the total destruction of the property. If the property is a structure, the maximum possible loss is the entire structure and all of its contents.

Step 4: Response Planning

Once risks have been identified, assessed, and ranked, management needs to determine the appropriate responses. In doing so, management will consider the risk of loss, the amount of loss, and the costs and benefits of the various risk responses. A company can choose among five responses for each specific risk:

1) **Avoid.** The company choses to eliminate the risky event or item. They might sell or otherwise disposing of a business unit or product line, or they might leave a specific geographic area. Efficiently deploying "avoid the risk" requires a great deal of foresight and fortitude, since the activity under

consideration may be extremely profitable. As a result, the problem with "avoid" is that it is usually considered only after a damaging risk event has already occurred.

2) **Reduce (mitigate).** Management recognizes that the risk will continue to exist but they look for ways to decrease its potential impact. They might expand an existing product line, split a function into two geographically separate areas, or diversify.

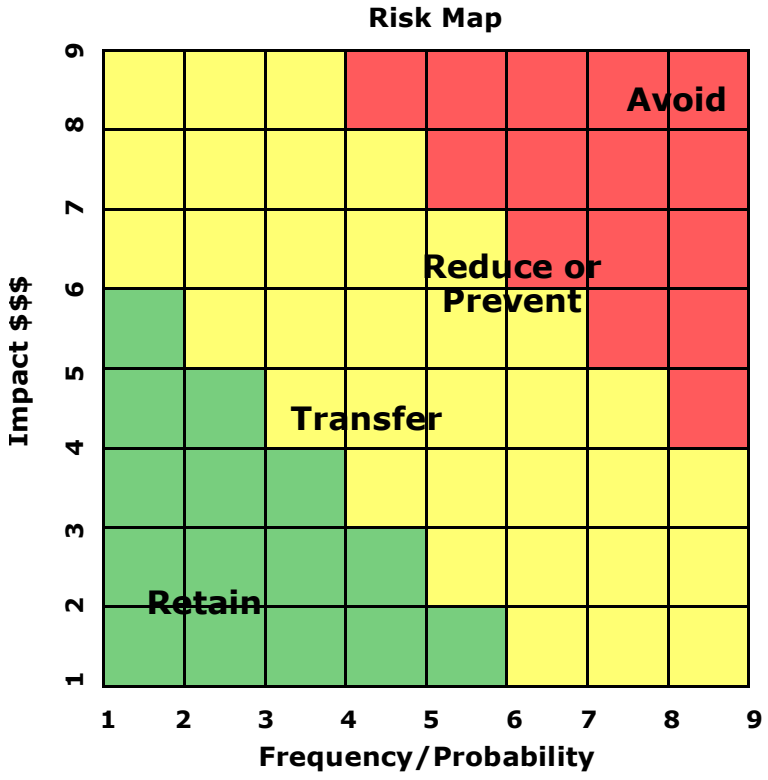
3) **Transfer (share).** Management transfers the risk of loss either partially or wholly to another organization. The primary example of transferred risk is purchasing insurance. Through insurance the company transfers risk to the insurance company. Risk can also be transferred through a contract or by using derivatives as hedges.

> **Note: Risk transfer is not risk prevention.** In other words, a company is not trying to prevent an unwanted event from occurring by purchasing insurance. Rather, it is **transferring the risk** of loss to another organization should that event occur. For example, if a company buys hurricane insurance, it is not preventing a hurricane. Instead, it is transferring the risk of hurricane-related loss from themselves to the insurance company.

4) **Retain**. Under certain circumstances, the company may wish to accept some or all of the impact of a risk. For example, a retained risk is the portion of a risk not covered by insurance, such as a deductible. A company can adjust the amount of retained risk by increasing or decreasing the deductible. A retained risk may also be a risk that the firm chooses to self-insure against; that is, the company elects to budget and pay for the risk out of its own funds.

5) **Exploit (accept).** Exploiting a risk is the strategic process by which a firm deliberately exposes itself to risk because management believes they can generate value for shareholders. For example, a company might invest in an emerging geographic market that carries substantial political and economic volatility or introduce a new product when its success is uncertain.

A risk map can help determine the appropriate response to each risk. The chart below includes the suggested risk response for each combination of impact and probability, depending upon where each risk is mapped.



After the risk management process has been completed, some **residual risk** may remain. Any residual risk should be reported to the appropriate level (for example, the board of directors) so that the company can decide either to accept the residual risk or reduce it further.

Question 5: Buckeye Conferencing leases meeting rooms to outside parties to use. The lease specifies that the outside party, not Buckeye Conferencing, will be liable for any damages resulting from the use of the meeting room, and that Buckeye Conferencing would be "held harmless" for these damages caused by the outside party. Buckeye Conferencing's actions demonstrate

a) Risk retention.

b) Self-insurance.

c) Insurance risk transfer.

d) Noninsurance risk transfer.

(HOCK)

Question 6: When the likelihood of loss is high and the amount at risk is high, the most appropriate risk response would probably be:

a) Avoiding the risk in whatever manner is available.

b) Reducing the risk by trying to minimize the loss that might occur.

c) Transferring the risk to another party through hedging or similar action.

d) Accepting the risk as the cost of reducing the risk will outweigh the potential benefits.

(HOCK)

Step 5: Risk Monitoring

After risk management strategies have been implemented, the company must ensure that each risk has been addressed. Additionally, an ongoing review and assessment of the risk management process is needed because what may have work in the past may no longer be relevant in the present.

Furthermore, external conditions can change. New risks may appear or an identified risk may become an even greater threat. For example, unexpected political events may arise, which may create new risks and increase its concern about a certain geographical area.

A senior manager responsible for the risk area might conduct follow-up risk management. These managers should be surveyed regularly or should report regularly with a current assessment on the likelihood of an identified risk occurring. In addition, internal auditors can ask about the status of identified risk areas as they perform their internal audits.

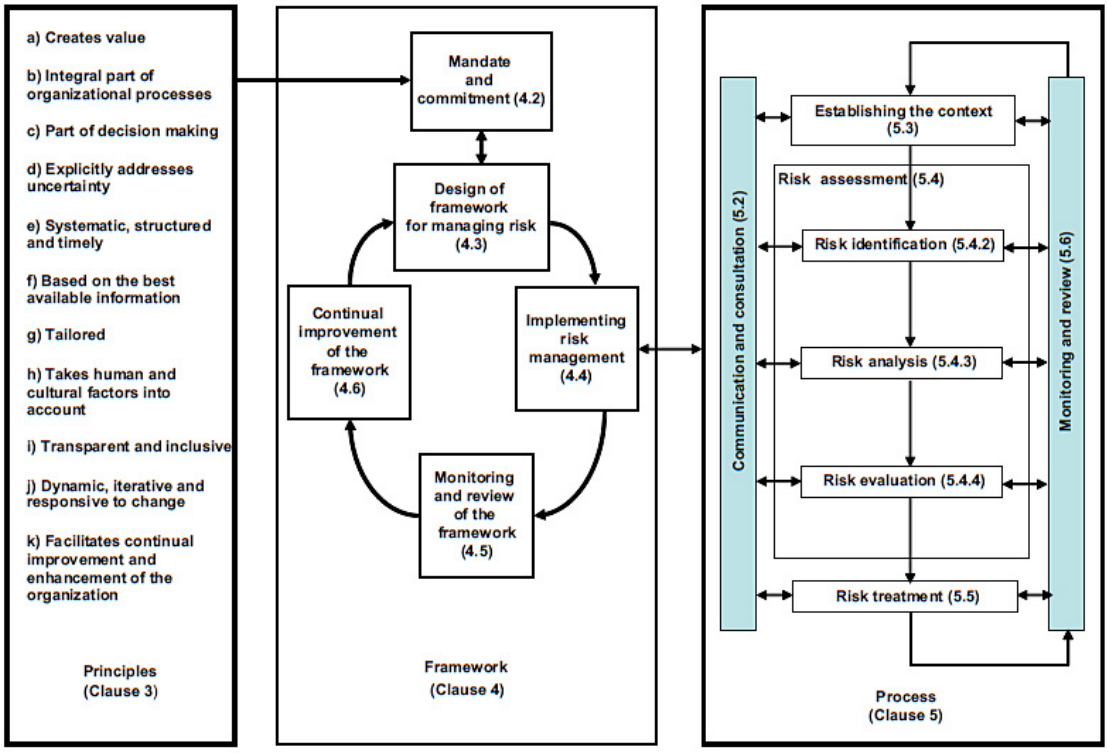
Note: A company's **risk appetite**, the amount of risk it is willing to accept in pursuit of value, will greatly influence its risk management process. A company's attitude toward risk may come from its shareholders, its contractual requirements, regulatory requirements, or the philosophy of its management.

Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake. Companies that are less tolerant of risk will identify more specific risks than a company that has a greater risk tolerance.

ISO 31000 Principles, Framework and Process

Having looked above at a general approach to risk management, we will now look at the process that is outlined in ISO 31000. It is very similar in overall approach, but some of the terms are different than what we have seen above.

Below is the diagram of the Principles, Framework, and Process of ISO 31000. The numerical references refer to the specific section of ISO 31000. This diagram is repeated at the end of this section.



ISO 31000 Principles of Risk Management (Clause 3 in the diagram)

ISO 31000:2009 identifies the following 11 principles that an organization should comply with at all levels in order for risk management to be effective:

1) **Risk management creates and protects value.** Risk management helps the company achieve its objectives and therefore it creates value. It also protects the current value of the business from loss.

2) **It is an integral part of all organizational processes.** Risk management does not operate in isolation. It needs to be part of all planning and all processes.

3) **It is part of decision making.** Risk management helps managers make informed decisions by providing information about alternative courses of action.

4) **It explicitly addresses uncertainty.**

5) **It is systematic, structured, and timely.**

6) **It is based on the best available information.** There are many situations in which more or better information is desirable. However, the lack of perfect information cannot prevent decisions from being made. Risk management uses the best available information.

7) **It is tailored.** What works for one company may not work for another. Risk management decisions must fit the specific needs of the given organization.

8) **It takes human and cultural factors into account.** Risk management must take into account the skills, knowledge, attitudes, and perceptions of individuals both within and outside the organization that will impact the risk management process.

9) **It is transparent and inclusive.** Risk management involves all relevant stakeholders and decision makers in a timely manner.

10) **It is dynamic, iterative, and responsive to change.** Risk management needs to continuously change as internal and external environments change. What may have been effective in the past may no longer be effective in the present.

11) **It facilitates continual improvement of the organization.** Risk management should strive for continuous maturity and improvement.

The ISO 31000 Framework (Clause 4 in the diagram)

The ISO 31000 Framework for risk management contains five steps:

1) Mandate and commitment
2) Design of framework for managing risk
3) Implementing risk management
4) Monitoring and review of the framework
5) Continual improvement of the framework

Exam Note: In the exam, if a question is specifically about ISO 31000, answer with the terminology specific to ISO 31000. If a question does not specifically mention ISO 31000 but includes ISO 31000 terminology, use the ISO 31000 terminology for answering the question. However, in addition to ISO 31000, you need to understand risk management as a general concept, which may not include ISO 31000 terminology.

1) Mandate and Commitment

Management plays a critical role in the risk management process, setting the tone and leading the process of adopting risk management throughout the organization through the following:

- Support the risk management policy.
- Ensure that the culture of the company and the risk management policy are in agreement.
- Set risk-management performance indicators that align with the company's performance indicators.
- Assign accountability and responsibility to the appropriate levels in the organization.
- Ensure that the needed resources are allocated and available to the risk management process.
- Communicate the benefits of the risk management process to all stakeholders.
- Ensure that the risk management framework stays relevant and appropriate over time.

2) Design of Framework for Managing Risk

Before risk management can take place, the organization must understand the **internal and external environments**, as they impact the design of the framework.

The evaluation of the **external environment** (also called **context**) should include (but is not limited to):

- Evaluating the social, cultural, political, legal, regulatory, financial, technological, economic, and competitive environment.

- Evaluating the relationships with external stakeholders, including their perceived values.
- Identifying external factors that may impact the achievement of the objectives.

The evaluation of the **internal environment** should include (but is not limited to):

- Evaluating the organization's culture, structure, and corporate governance.
- Analyzing objectives along with the policies and procedures in place to achieve them.
- Examining the company's capabilities, including capital, time, and human resources.
- Appraising the relationships with internal stakeholders, including the perceived values that each holds.

The organization also must **establish a risk management policy**. It should state the organization's objectives for risk management, as well their commitment to risk management. This policy should include:

- The rationale for managing risk.
- The accountabilities and responsibilities for managing risk, which also means identifying who is responsible for the development, maintenance, and implementation of the risk framework.
- A mechanism to address conflicts of interest.
- A **commitment to make the needed resources available** to assist those who are accountable and responsible for risk management. These resources include people, information, management systems, and training programs.
- The manner in which risk management will be measured and reported.
- Internal and external communication and reporting mechanisms.

After the risk management policy has been completed, there are two important actions that must be done. First, the policy must be communicated to all those who it affects. Second, risk management must be embedded into all organizational processes, from top to bottom.

3) Implementing Risk Management (Including Risk Assessment)

Note: This implementation is called the **Process** in ISO 31000 (Clause 5 in the diagram).

While all steps of risk management are critical, **implementing risk management is at the heart of the process**. The three main steps in implementing risk management are:

3A) Establishing the context

3B) Risk assessment

3C) Risk treatment

Accompanying these three steps are two supporting activities:

3D) Communication and consultation

3E) Monitoring and review

3A) Establishing the Context

When the organization establishes the context of risk management, it is determining its objectives and identifying the internal and external elements of the environment that need to be taken into account when managing risk. It also sets the scope and criteria for the remainder of the risk management process. The risk criteria should reflect the organizations values, objectives, and resources, which is the basis for the risk treatment decisions that need to be made later.

3B) Risk Assessment

The following list outlines the three stages of risk assessment with a few added elaborations with respect to ISO 31000:

1) **Risk identification.** All internal and external risks must be identified in order to address all threats that the organization faces.
2) **Risk analysis.**
3) **Risk evaluation.** The level of assessed risk is compared to the risk criteria, thereby giving guidance for appropriate treatment.

3C) Risk Treatment

Risk treatment is the process of selecting one or more responses to risk and then implementing them. Risk treatment also includes assessing residual risk to determine if it is acceptable. A final step is assessing the effectiveness over time of the selected risk treatment options.

ISO 31000 lists seven risk treatment options, though they are not the only options available.

1) **Avoiding** the risk, either by not starting the risky activity or discontinuing it.
2) **Taking on or increasing** the risk to take advantage of an opportunity.
3) **Removing** the risk source.
4) **Changing the likelihoods** of the different possible outcomes.
5) **Changing the consequences** of the different outcomes.
6) **Sharing** the risk with other parties.
7) **Retaining** the risk, after making an informed decision.

In choosing the correct response or responses, management must carefully balance the costs and benefits of each option. Individual risk responses may cause other risks, which in turn should be identified and assessed. Additionally, the company needs to assess the residual risk. Further actions may still need to be taken if the residual risk is unacceptably high.

3D) Communication and Consultation

Communication and consultation with internal and external stakeholders should take place during all stages of the risk management process. Ongoing communication will ensure that stakeholders will understand the basis on which decisions have been made and the reasons that specific actions are required.

3E) Monitoring and Review of Risk Management Process

Monitoring and review should be a part of the risk management process, including both scheduled and regular reviews as well as any additional reviews should the internal and external environments change. The results of the reviews should be recorded and then communicated as appropriate, both internally and externally.

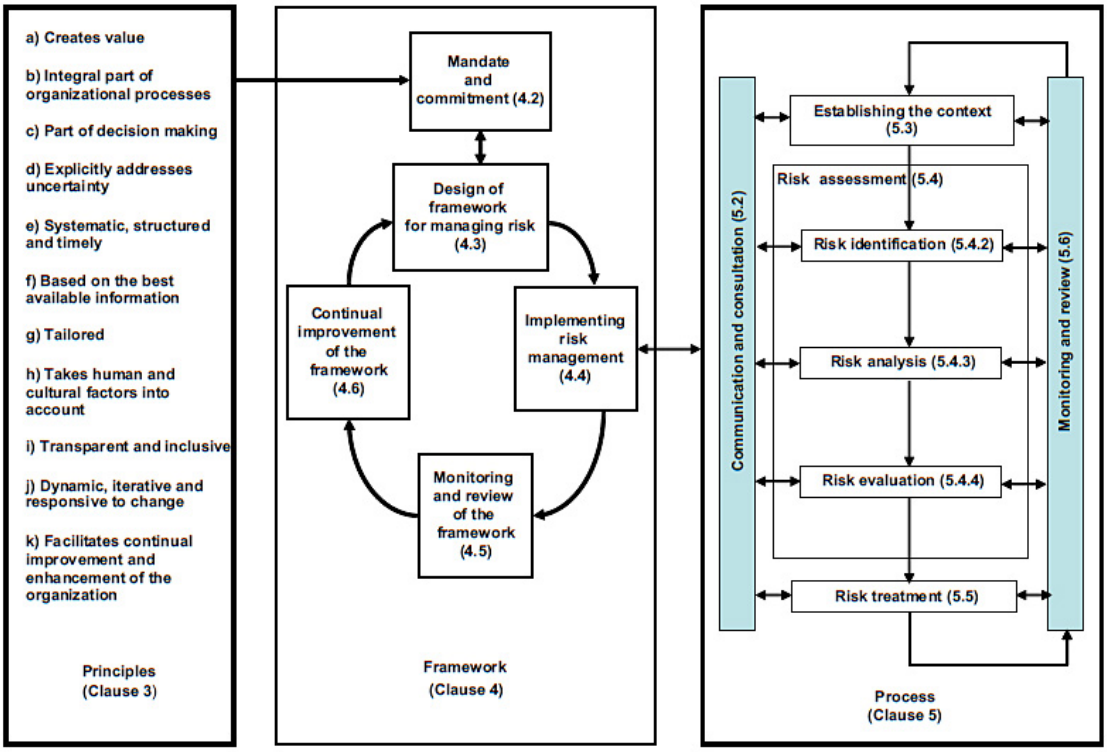
4) Monitoring and Review of the Framework

To assess the effectiveness of the risk management process, the organization should measure risk performance against indicators. They should also measure the risk management process against the risk management plan. Any deviations from the plan should be investigated to identify any issues that need to be corrected. Additionally, the organization should periodically—probably on an annual basis—assess the risk management framework, policy, and plan to make sure they are still appropriate given any changes in the external and internal environments.

5) Continual Improvement of the Framework

The results of the monitoring and reviews in Step 4 should produce guidance for improving the risk management framework, policy, and plan. As these improvements are implemented, the organization's risk management and internal culture should improve. Therefore, this process needs to be done at regular intervals because the business environment is ever changing and dynamic.

Below is the diagram of the Principles, Framework, and Process of ISO 31000. The numerical references refer to the specific section of ISO 31000.



IIB. Organizational Use of Risk Frameworks – ERM

Note: The main source for information about ERM is the document entitled "Enterprise Risk Management – Integrated Framework." This document was published in 2004 by the Committee of Sponsoring Organizations (COSO)[10]. A number of other organizations also have comprehensive guidance about ERM systems. The ICMA's Learning Outcome Statements specify the use of the COSO document, so that is the reference used in the following.

As defined by COSO,

> "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may effect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding achievement of entity objectives."

[10] The Committee of Sponsoring Organizations (COSO) is the Committee of Sponsoring Organizations of the National Commission on Fraudulent Financial Reporting (called by the popular name "Treadway Commission" after its original chairman, James C. Treadway, Jr.). The Treadway Commission was formed in 1985 by and was funded by the five main professional accounting associations in the U.S.: the American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Institute, Institute of Management Accountants, and The Institute of Internal Auditors.

Answers to Questions

1 d – Legal risk includes the legal system in which the company operates and the risks of losses from legal cases.

2 c – Operational risks are risks that that result from inadequate or failed internal processes, people or systems. Failure to perform bank reconciliations for six months is an example of a failed internal process.

3 a – Riverfront was not in compliance with laws and regulations. The owner has created compliance risk, which is operational risk. Compliance risk is the current or future risk to profits or the company's assets as a result of violations of, or nonconformance with, laws, rules, regulations, required practices, internal policies and procedures, or ethical standards. While it is true that the remaining inspections could determine that the building is uninhabitable, the risk created is compliance risk that is due to noncomformance with laws requiring satisfactory inspections and a certificate of occupancy before allowing tenants to move in.

4 d – Value at risk provides a confidence interval which provides a range of results with a percentage chance that the result will be within that range.

5 d – By moving the risk away from themselves to another party, Buckeye Conferencing is transferring the risk of loss to another party, though insurance is not involved. This is a noninsurance risk transfer.

6 a – When the risk of loss is high and the likelihood is high, the best course of action is probably to avoid the risk. This might include selling the business unit or in some other way eliminating the risk-generating activity from the company.

7 b – Corporate governance is concerned with the achievement of the corporation's objectives. Enterprise Risk Management assists the organization in the achievement of its objectives because it identifies the organizations' objectives that are at risk. Therefore, Enterprise Risk Management is aligned with corporate governance.

8 a – Supply chain disruption is a common risk, and it entails both inherent and residual risk. Suppliers do have problems and can sometimes be unable to supply a product, perhaps because of production difficulties or because of problems getting product from their own suppliers. The risk is inherent because occasional difficulty in obtaining a product is just a natural part of the process of ordering. As a response to the risk of supply chain disruption, a company should make sure it has more than one supplier at all times for every item it uses. However, even if the company has several suppliers, some residual risk still remains. For example, if only one manufacturer is producing an item and that manufacturer has production problems, all of the company's suppliers will be unable to obtain that item and thus none of them may be able to fulfill a given order.

9 a – The risk management philosophy of the company, the attitude toward risk of its Board of Directors, and the integrity and ethical values that make up the culture of the company are all parts of the internal environment. Control activities are a separate component of ERM.

10 a – The proper order for the four ERM components given is objective setting, event identification, risk assessment, risk response.

11 b – Sales representatives are in constant contact with customers, so they would be in the best position to recognize a problem related to customer product design. The other people named do not have contact with customers.

12 b – In any delegation, it is critical that the task or outcome be precisely defined. Additionally, it is good if there is discussion about how it will be done. The manager does not want to dictate how it should be done and also should not let the subordinate decide how it will be done, because that may lead to a lot of wasted time and resources if the subordinate chooses an inappropriate method for completing the task.

13 b – A mechanistic approach is used when there is an assembly line type system where there is not a need for a lot of decision-making. This system is motivated by efficiency and trying to produce as much as possible.

14 a – In a dynamic and complex environment, the company will face more uncertainty because the environment is changing. As a result, it will need a more organic structure in order to react better to the changes.

15 c – Discount stores gain their market edge by selling at a lower price and therefore need to minimize their costs. This is done by not offering as much sales help or the more "decorated" stores as their competitors provide.

16 a – As companies grow, they tend to expand their efforts and the products or services they offer. Their expansion may also be outside of their initial industry as well as within it.

17 c – By definition, in a professional bureaucracy, management has to give up a lot of control.

18 c – A bureaucratic structure does not allow for much creativity. This is one of the disadvantages of this structure.

19 b – In a divisional structure, each division may have its own staff to perform a function that all divisions have. An example may be payroll or HR. Each division may have its own payroll or HR department, and as such, the company as a whole has duplicate departments.

20 b – In a matrix organization, there is a combination of organizational methods. As such, an employee may end up reporting to a functional manager as well as to a project team manager, or other multiple managers.

21 d – The number of people in an organization does not impact the span of control that a manager would have.

22 c – Generally, if the jobs are fairly similar and procedures are alike, then a wider span of control would be most effective.

23 d – The internal auditor should not become directly involved in the implementation of the redesign process. The internal auditor's direct involvement would impair the auditor's objectivity and independence.

24 d – Customer service, production, marketing and sales, and R&D are the primary activities or business functions that add value to a company's product or service. Information systems, infrastructure, human resources, and materials management are activities that support these primary activities as defined in the value chain.

25 d – Because the analysis is to include identifying where customer value can be increased, the type of analysis the consultant most likely has been asked to perform is a value-chain analysis.

26 a – E-commerce does not relate to data storage.

27 a – An audit trail allows for tracing of transactions from initiation to conclusion.

28 c – EDI is the electronic transfer of documents between businesses.

29 b – In the growth stage, if an entity is reasonably profitable, then it could need financing in excess of the funds it has available from internal sources (i.e. trade receivables). Additional debt financing could result in unreasonable financial leverage and public equity financing is generally not yet available. Therefore, a company in the growth stage is most likely to seek and obtain venture capital.

30 b – Communication is dependent upon the receiver understanding the message properly. If the receiver does not understand it, then communication has not taken place.

31 c – When formal communication is insufficient, rumors will fill the gap due to employees' anxiety and desire to know what is happening. Such a situation may have a negative effect on morale and reduce the employees' productivity.

32 c – The medium chosen by the clerk was wrong because there is no written record of the telephone order to substantiate any claim, as there would have been if a purchase order had been issued.

33 b – The only acceptable way to let an employee know that their employment is being terminated is face to face.

34 b – Filtering is presenting information in such a way that it will be received favorably.

35 b – Many different issues within a short time period will impede comprehension and is therefore unlikely to lead to desired changes in attitudes.

36 d – An effective communicator has to take into account the receivers' needs and opinions to make sure that they do not interfere with the message and the message is received and understood properly.

37 a – Effective listening is best achieved by resisting internal and external distractions. Distractions, i.e. noise, make it more difficult for the listener to truly understand the message.

38 a – Information overload and misrepresentation of feelings and emotions are considered to be disadvantages of electronic communication. Information overload, such as numerous irrelevant memos, could lead to lost time and inefficiencies. Also, email cannot accurately convey feelings and tone intended by the person initiating the communication. Thus, the receiver may misinterpret the email.

39 b – Market synergy is a type of business synergy. It arises when products or services positively complement each other. The bundling of products distributed through the same channels is a type of market synergy.

40 b – A focus strategy seeks to be a cost leader in a particular segment. The theory behind the focus strategy is that a narrow market can be better served.

41 b – Threat of new entrants and bargaining power of suppliers are two of the five basic forces that drive industry competition and ultimately profitability. The other three forces are rivalry, bargaining power of buyers, and threat from substitutes.

