Assignment 2

Introduction to Risk Management Standards and Guidelines

Educational Objective (EO)

Describe the general characteristics and elements of risk management standards and guidelines.

Instructions

Activity 1 — Describing Risk Management Standards and Guidelines

Individual Activity Followed by Large Group Discussion

Ask participants to complete the questions in **Activity 1—Describing Risk Management Standards and Guidelines**.

Alternatively, this activity could be assigned as pre-work. If used as an assignment, have participants come prepared to share their answers in class.

Debrief:

Reconvene the large group and ask for volunteers to share their answers.

Activity 1 — Describing Risk Management Standards and Guidelines

Questions	Answers
1. Describe the framework.	
2. What must an organization do to implement a successful risk management program?	
3. How does the definition of risk differ between ISO 31000 and Committee of Sponsoring Organizations' enterprise risk management?	
4. List the criteria that a risk management process should be based on for a successful implementation.	
5. What are the essential attributes that the Risk Maturity Model focuses on?	

Answers to Activity 1 — Describing Risk Management Standards and Guidelines

Questions	Answers
1. Describe the framework.	The framework is the structure that supports the organization's objectives and strategies. It provides the scaffold that an organization uses to construct and maintain its risk management process.
2. What must an organization do to implement a successful risk management program?	An organization must select the standard that will align with the organization's mission, values, objectives, and corporate structure.
3. How does the definition of risk differ between ISO 31000 and Committee of Sponsoring Organizations' enterprise risk management?	• COSO—The "possibility that an event will occur and adversely affect the achievement of objectives." This definition reflects the traditional meaning of risk—namely, that it represents the potential only for adverse results. • ISO 31000—"the effect of uncertainty on objectives." This definition reflects more recent thinking about risk, which encompasses the potential for positive as well as adverse results.
4. List the criteria that a risk management process should be based on for a successful implementation.	• Alignment with organizational objectives • Adherence to controls • Need to meet regulatory requirements (compliance) • Risk governance
5. What are the essential attributes that the Risk Maturity Model focuses on?	• ERM-based approach • ERM process management • Risk appetite management • Root cause discipline • Uncovering risks • Performance management • Business resiliency and sustainability

ISO 31000 Risk Management—Principles and Guidelines

Educational Objective (EO)

Explain how ISO 31000 provides a framework and a process for an organization to manage its risks.

Instructions

Activity 1 — Describing Framework and Process of ISO 31000

Individual Activity Followed by Large Group Discussion

Ask participants to complete the questions in **Activity 1— Describing Framework and Process of ISO 31000**.

Alternatively, this activity could be assigned as pre-work. If used as an assignment, have participants come prepared to share their answers in class.

Debrief:

Reconvene the large group and ask for volunteers to share their answers.

Activity 1 — Describing Framework and Process of ISO 31000

Questions	Answers
1. How does the ISO 31000 framework help organizations?	
2. What must be in place to ensure a successful implementation of a risk management framework in an organization?	
3. List the seven components of a risk management framework.	
4. What are risk criteria?	
5. What are the three major phases of the risk management process?	
6. Describe the three steps in risk assessment.	
7. Describe risk treatment	

Questions	Answers
8. What is included in the monitoring and reporting phase of the risk management process?	

Answers to Activity 1 — Describing Framework and Process of ISO 31000

Questions	Answers
1. How does the ISO 31000 framework help organizations?	Integrate the risk management process into management and operational systems.
2. What must be in place to ensure a successful implementation of a risk management framework in an organization?	A strong mandate and commitment from managers.
3. List the seven components of a risk management framework.	- Evaluate - Establish policy - Accountability - Integrate - Resources - Establish internal communications - Establish external communication
4. What are risk criteria?	Terms of reference against which the significance of a risk is evaluated.
5. What are the three major phases of the risk management process?	- Risk assessment - Risk treatment - Monitoring
6. Describe the three steps in risk assessment.	- Identify risks—It is important to identify as many risks as possible, prioritizing the key risks in terms of their effect on the organization's objectives. - Analysis—quantitative, qualitative, or a combination of the two. This analysis includes determining the level of risk and its potential effect on the organization. Both the tangible and intangible effects of consequences should be considered. - Evaluate organization's risks—applying the selected risk criteria to the levels of risk determined during the analysis.
7. Describe risk treatment	The ongoing process of deciding on an option for modifying risk and whether the retained level of risk is acceptable, selecting a new risk treatment if the current one is not effective, and then repeating this assessment.

Questions	Answers
8. What is included in the monitoring and reporting phase of the risk management process?	• Assessment of both internal and external changes and how these changes affect risks and their treatment. • Recording the assessments and reporting them internally and externally to those who need the information. • Determining the frequency, distribution, and method of reporting is an integral part of developing the risk management process.

COSO Enterprise Risk Management—Integrated Framework

Educational Objective (EO)

Explain how the Committee of Sponsoring Organizations' Enterprise Risk Management—Integrated Framework provides a standard by which an organization can manage its risks.

Instructions

Activity 1 — Explaining COSO ERM Integrated Framework and Control Activities

Game or Large Group Activity

Divide participants into small groups (teams). Using two flipchart pages (or dry erase boards), draw the "Integrated Framework" table on one flipchart and the "Control Activities" table on the other flipchart as shown in **Activity 1—Explaining COSO ERM Integrated Framework and Control Activities.**

Post the tables so everyone can access them. The game part of the activity is a "round robin tournament." Call on a team participant in turn to write a fact in either of the tables. For example, a team participant might write "Strategic" on the "Integrated Framework" flipchart in the "Objectives Categories" column. The next participant might write the description for "Strategic" or could write a fact for Control Activities. You might need more than one sheet of paper for some of the steps in the process.

Team participants cannot duplicate what someone else has written. If a team participant cannot come up with anything to write, that team participant is eliminated from the tournament. Continue in this manner until you have only one team left and you can declare a winner.

Debrief:
If necessary, review the answers provided with the class.

Activity 1 — Explaining COSO ERM Integrated Framework and Control Activities

COSO ENTERPRISE RISK MANAGEMENT—INTEGRATED FRAMEWORK	
Objectives Categories	**Description**
1.	
2.	
3.	
4.	
Interrelated components	**Description**
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	

CONTROL ACTIVITIES	
Control Activity Part	**Description**
1.	
2.	
Control Activity Monitoring	**Description**
1.	
2.	

Solvency II and Basel II and III Regulatory Standards

Educational Objective (EO)

Explain how the Solvency II and Basel II and III regulatory standards apply to the insurance and banking industries, respectively.

Instructions

Activity 1 — Describing Solvency II and Basel II and III Regulatory Standards

Game or Large Group Activity: The Amazing Race

Divide participants into two groups to form teams. Assign each team a regulatory standard that they will represent, either "Solvency II" or "Basel II and III." Label two flipchart pages, one as "Solvency II" and the other "Basel II and III." More flipchart pages may be needed.

Post the flipchart pages on the wall or dry erase board. The game part of the activity is a timed race. Each team races to complete as much information as possible for their assigned group. Only one team participant can go to the chart to write a *key fact* about their regulatory standard, return to their group and pass the marker to the next participant. Team participants cannot duplicate anything else that has been written by another team participant.

Begin the game and start the timer. After 15 minutes, tell the teams to stop writing. The team that provided the most information for their assigned group within the allotted time is declared the winner.

If there is a tie, use these questions as bonus points to declare a winner (or use to engage participants in discussion):

1. What is the goal Solvency II and Basel III regulatory standards?
2. Name a risk management standard that is voluntary.
3. [Blank] is a new regulatory standard for insurers in the European Union (EU) to establish principles for risk management and consistency in regulation.
4. [Blank] is the new regulatory standard for the global banking industry that sets out risk management principles designed to prevent systemic risk from creating another financial crisis similar to the one that occurred in 2007.

Debrief:
Review the responses for each group with the class. Use the questions to engage the participants in discussion.