Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://www.fast2test.com

Everything you need to prepare, learn & pass your certification exam easily.

Exam : **ISO-31000-Lead-Risk-Manager**

Title : PECB ISO 31000 Lead Risk Manager

Vendor : PECB

Version : DEMO

QUESTION NO: 1
A risk manager wants to improve organizational resilience by embedding climate-related considerations into performance measures, while also fostering open communication about risks across all levels of the organization. Which of the following practices are they considering?
A. Commitment to ongoing learning and strengthening of collaboration
B. Integration of sustainability and promotion of risk culture
C. Adoption of new technologies and focus on compliance
D. Risk avoidance and risk transfer strategies
Answer: B
Explanation:
The correct answer is B. Integration of sustainability and promotion of risk culture. ISO 31000 emphasizes that risk management should be integrated into organizational activities, including performance management, decision-making, and strategic planning. Embedding climate-related considerations into performance measures reflects the integration of sustainability-related risks into the organization's risk management and performance framework.
At the same time, fostering open communication about risks across all organizational levels aligns with the development and promotion of a positive risk culture, which ISO 31000 identifies as a key enabler of effective risk management. A strong risk culture encourages transparency, awareness, and proactive engagement with risk, supporting resilience and informed decision-making.
Option A focuses on learning and collaboration, which are important but do not directly address sustainability integration and risk culture. Option C emphasizes technology and compliance, which are supporting elements but not the core practices described. Option D refers to specific risk treatment options rather than organizational practices aimed at resilience.
From a PECB ISO 31000 Lead Risk Manager perspective, integrating sustainability considerations and promoting a strong risk culture enhances the organization's ability to anticipate, respond to, and adapt to evolving risks such as climate change. Therefore, the correct answer is integration of sustainability and promotion of risk culture.

QUESTION NO: 2
On what basis should an organization determine the acceptability of a residual risk?
A. A risk is acceptable only when its residual level is higher than the target risk to allow flexibility in controls.
B. The target risk must always be set at a low level to ensure that all residual risks are minimized.
C. A residual risk is accepted when it is equal to or below the target risk.
D. A residual risk is accepted when treatment costs exceed potential benefits.
Answer: C
Explanation:
The correct answer is C. A residual risk is accepted when it is equal to or below the target risk. ISO 31000:2018 explains that risk treatment aims to modify risk so that it aligns with the

organization's risk criteria, which include risk appetite, tolerance, and target risk levels. Residual risk is the risk remaining after risk treatment has been applied.
An organization determines acceptability by comparing the residual risk against predefined target risk or risk acceptance criteria. When the residual risk falls within acceptable limits, meaning it is equal to or lower than the target risk, it may be accepted without further treatment. This ensures consistency, transparency, and alignment with strategic objectives.
Option A is incorrect because accepting risks higher than the target risk contradicts the purpose of risk criteria. Option B is incorrect because target risk levels vary depending on objectives, context, and appetite; they are not always low. Option D may influence decision-making but is not the formal basis defined by ISO 31000.
From a PECB ISO 31000 Lead Risk Manager perspective, clear acceptance criteria ensure disciplined and defensible risk decisions. Therefore, the correct answer is a residual risk is accepted when it is equal to or below the target risk.

QUESTION NO: 3
Scenario 4:
Headquartered in Barcelona, Spain, Solenco Energy is a renewable energy provider that operates several solar and wind farms across southern Europe. After experiencing periodic equipment failures and supplier delays that affected energy output, the company initiated a risk assessment in line with ISO 31000 to ensure organizational resilience, minimize disruptions, and support long-term performance.
A cross-functional risk team was assembled, including representatives from engineering, finance, operations, and logistics. The team began a structured and systematic review of the energy production process to identify potential deviations from intended operating conditions and assess their possible causes and consequences. Using guided discussions with prompts such as "too high," "too low," or "other than expected," they explored how variations in system behavior could lead to operational disruptions or safety risks.
One risk identified was the failure of the main power inverter system at one of the company's key solar facilities-a single point of failure with high production dependence. To better understand this risk, the team used a structured visual technique that mapped the causes leading up to the inverter failure on one side and the potential consequences on the other. It also illustrated the controls that could prevent or mitigate both sides.
During discussions, several team members were inclined to focus on positive evidence supporting the belief that the inverter was reliable, while giving less consideration to contradictory data from maintenance reports. Differing viewpoints were not immediately discussed, as many participants felt more confident agreeing with the general group view that the likelihood of failure was low. It was only after a detailed review of supplier reports that the team revisited their assumptions and adjusted the analysis accordingly.
Ultimately, the likelihood of failure was determined to be "possible" based on annual system monitoring and maintenance records. However, the consequences were potentially severe, including an estimated €450,000 in lost revenue per week of downtime, contract penalties, and negative stakeholder perceptions. The team assumed a potential downtime of two weeks per failure, resulting in a total potential loss of €900,000 per event.
To better quantify the financial exposure to this risk, the team multiplied the estimated probability of failure (10%) by the potential loss per event (€900,000), yielding an annual expected impact of €90,000. This calculation provided a clearer basis for prioritizing the

inverter failure risk relative to other risks in the risk register.
Based on the scenario above, answer the following question:
What did the team at Solenco determine when they examined the likelihood and consequences of the inverter failure?

A. The level of risk

B. The criteria for risk acceptance

C. Risk tolerance

D. Risk appetite

Answer: A

Explanation:
The correct answer is A. The level of risk. ISO 31000:2018 defines risk level as the magnitude of a risk, commonly expressed as a combination of the likelihood of an event and its consequences. Determining the level of risk is a core outcome of risk analysis, which aims to develop an understanding of the nature of risk and its characteristics.
In Scenario 4, the Solenco team explicitly assessed both the likelihood ("possible," quantified as 10%) and the consequences (€900,000 per event) of inverter failure. They then combined these elements by calculating an expected annual impact of €90,000. This quantitative combination of likelihood and consequence directly represents the determination of the level of risk, enabling comparison and prioritization within the risk register.
Risk acceptance criteria and risk tolerance relate to decision-making thresholds that determine whether a risk is acceptable or requires treatment. These are defined earlier during context establishment and risk criteria setting, not calculated during risk analysis. Risk appetite refers to the amount and type of risk an organization is willing to pursue and is a strategic-level concept, not a calculated outcome of likelihood and consequence.
From a PECB ISO 31000 Lead Risk Manager perspective, calculating the level of risk supports informed risk evaluation and prioritization. It enables organizations to allocate resources effectively and focus on risks that threaten value creation and protection.
Therefore, the correct answer is the level of risk.

QUESTION NO: 4
According to ISO 31000, how can top management and oversight bodies demonstrate their commitment to risk management?

A. By developing and communicating a clear policy that expresses the organization's objectives and commitment to risk management

B. By avoiding formal documentation to maintain flexibility in risk management practices

C. By relying on external experts to handle all risk-related matters

D. By delegating all risk responsibilities to operational managers

Answer: A

Explanation:
The correct answer is A. By developing and communicating a clear policy that expresses the organization's objectives and commitment to risk management. ISO 31000:2018 places strong emphasis on leadership and commitment as a foundational element of the risk management framework. Top management and oversight bodies are expected to demonstrate commitment by establishing direction, ensuring alignment with organizational

objectives, and visibly supporting risk management activities.
ISO 31000 explicitly states that leadership commitment should be demonstrated through actions such as issuing a risk management policy, allocating resources, assigning responsibilities, and ensuring integration of risk management into governance and decision-making. A clearly communicated policy provides a common understanding of the organization's approach to risk, reinforces expectations, and promotes consistent behavior across all levels.
Option B is incorrect because ISO 31000 does not advocate avoiding documentation. While flexibility is important, formal documentation such as policies and frameworks is necessary to ensure clarity, consistency, and accountability. Option C is incorrect because reliance on external experts does not replace leadership responsibility; risk management accountability remains with the organization. Option D is also incorrect, as delegation without leadership involvement contradicts ISO 31000's emphasis on top management responsibility.
From a PECB ISO 31000 Lead Risk Manager perspective, visible and documented commitment by leadership is essential for embedding risk management into organizational culture and operations. Therefore, option A is correct.

QUESTION NO: 5
A company sets the objective "increase the number of internal risk reports submitted each quarter by staff," but it does not define the expected increase or how progress will be tracked. Which SMART criterion is missing in this objective?
A. Measurable
B. Relevant
C. Achievable
D. Time-bound
Answer: A
Explanation:
The correct answer is A. Measurable. ISO 31000 emphasizes that objectives should be clearly defined to support effective risk management, monitoring, and review. The SMART framework-Specific, Measurable, Achievable, Relevant, and Time-bound-is commonly used to ensure that objectives are well formulated and actionable.
In the given objective, the organization intends to increase the number of internal risk reports submitted each quarter. While the objective is specific and time-bound ("each quarter"), it lacks measurability because it does not define how much of an increase is expected or how success will be measured. Without quantitative targets or defined metrics, it becomes difficult to monitor progress, assess effectiveness, or trigger corrective actions.
Relevance is present, as increasing risk reporting supports a stronger risk culture and better risk identification. Achievability cannot be assessed fully, but the main deficiency highlighted is the absence of measurable criteria.
From a PECB ISO 31000 Lead Risk Manager perspective, measurable objectives are essential for evaluating whether risk management activities deliver intended outcomes. Without measurable indicators, monitoring and continual improvement become ineffective. Therefore, the correct answer is measurable.

QUESTION NO: 6

Scenario 7:
Maxime, a chocolate manufacturer headquartered in Ghent, Belgium, produces toffees, eclairs, enrobed chocolates, and caramels. In 2023, a contamination incident in its caramel line triggered a large-scale product recall across Europe, exposing weaknesses in supplier evaluation, reporting channels, and crisis communication. Recognizing the financial, operational, and reputational impact of this event, top management decided to apply a risk management process in line with ISO 31000. The aim was to strengthen resilience, embed risk awareness across departments, and ensure risks are systematically managed in both daily operations and long-term strategies.
To ensure that the risk management process is effective, Maxime set up a structured monitoring and review process with clear procedures for collecting and analyzing data on key risks like supplier reliability, food safety, and communication. For validation of measurement methods, Sophie, the head of Quality Assurance, was tasked with assessing whether the tools used were suitable for evaluating the effectiveness of the process.
Additionally, Maxime introduced a set of measures designed to provide early warning indicators across critical areas. In operations, they tracked the number of production line stoppages and the percentage of defective batches. On the financial side, they monitored fluctuations in raw material prices, especially cocoa, and their impact on margins. For regulatory matters, they followed the frequency of nonconformities identified during inspections. In terms of technology, system downtime in automated packaging lines was measured.
To ensure these indicators were communicated effectively, Sophie worked with top management to present the results in a format that made changes easy to spot and understand. Rather than relying only on static reports, they chose a more dynamic approach that displayed key values visually, highlighted deviations, and issued alerts when thresholds were crossed.
In addition, Maxime established clear communication and consultation processes to ensure that relevant stakeholders were properly engaged. The top management used an approach that clarified who was responsible for carrying out tasks, who held final accountability, who should be consulted for expertise, and who needed to stay informed. To strengthen engagement, Maxime organized how risk information would be delivered to different audiences. Employees received updates during team briefings and through the company's internal platform, while external parties, such as suppliers and regulators, were informed through formal reports and direct correspondence. This approach ensured that each group had access to the information most relevant to them in a timely way.
Based on the scenario above, answer the following question:
Which communication principle did Maxime adhere to by organizing how information was delivered to employees, suppliers, and regulators? Refer to Scenario 7.

A. Content

B. Context

C. Channels

D. Frequency

Answer: C

Explanation:
The correct answer is C. Channels. ISO 31000 states that communication should be timely,

appropriate, and tailored to the audience, ensuring that information is delivered through the most suitable means.
In Scenario 7, Maxime deliberately organized how risk information was delivered to different stakeholder groups. Employees received updates through team briefings and internal platforms, while suppliers and regulators were informed through formal reports and direct correspondence. This clearly reflects the communication principle of selecting appropriate channels.
Content relates to what information is communicated, and context refers to the environment or circumstances in which communication occurs. The scenario specifically emphasizes the delivery mechanisms, not the message itself or its broader context.
From a PECB ISO 31000 Lead Risk Manager perspective, selecting appropriate communication channels improves understanding, engagement, and responsiveness, particularly in risk-related matters. Therefore, the correct answer is Channels.

QUESTION NO: 7
Scenario 6:
Trunroll is a fast-food chain headquartered in Chicago, Illinois, specializing in wraps, burritos, and quick-serve snacks through both company-owned and franchised outlets across several states. Recently, the company identified two major risks: increased dependence on third-party delivery platforms that could disrupt customer service if contracts were to fail or fees rose sharply, and stricter health and safety inspections that might expose vulnerabilities in hygiene practices across certain franchise locations. Therefore, the top management of Trunroll adopted a structured risk management process based on ISO 31000 guidelines to systematically identify, assess, and mitigate risks, embedding risk awareness into daily operations and strengthening resilience against future disruptions.
To address these risks, Trunroll outlined and documented clear actions with defined responsibilities and timelines. Regarding the dependence on third-party delivery platforms, the company decided not to move forward with planned partnerships with third-party delivery apps, as the risk of losing control over the customer experience and rising costs outweighed the potential benefits.
To address stricter health inspections across franchises, Trunroll invested in stronger hygiene protocols, mandatory staff training, and upgraded monitoring systems to reduce the likelihood of violations. Yet, management understood that some exposure would remain even after these measures. To address this risk, they decided to use one of the insurance methods, reserving internal financial resources to cover unexpected losses or penalties, ensuring the remaining risk was managed within acceptable boundaries.
Additionally, Trunroll set up a cloud-based platform to document and maintain risk records. This allowed managers to log supplier inspection results, training outcomes, and incident reports into one secure system, while also providing flexibility to update and scale applications as needed without managing the underlying infrastructure. In doing so, Trunroll ensured that all risk-related information is documented in progress reports and incorporated into mid-term and final evaluations, with risk management being updated regularly to monitor changes and treatments.
Based on the scenario above, answer the following question:
According to Scenario 6, Trunroll outlined and documented clear actions to address the identified risks with defined responsibilities and timelines. What did they develop in this case?

A. A risk report
B. A risk treatment plan
C. A risk register
D. A risk policy
Answer: B
Explanation:
The correct answer is B. A risk treatment plan. ISO 31000 defines a risk treatment plan as a documented set of actions specifying how selected risk treatment options will be implemented, including responsibilities, timelines, and required resources.
In Scenario 6, Trunroll explicitly outlined and documented clear actions with defined responsibilities and timelines to address identified risks. These actions included avoiding third-party delivery partnerships, strengthening hygiene controls, investing in staff training, upgrading monitoring systems, and reserving internal financial resources to manage residual risk. These characteristics directly align with ISO 31000's definition of a risk treatment plan.
A risk report focuses on communicating risk information and decisions, not implementation actions. A risk register is a structured record of identified risks and their attributes but does not by itself define treatment actions, responsibilities, or schedules. A risk policy sets overall direction and commitment rather than operational actions.
From a PECB ISO 31000 Lead Risk Manager perspective, a risk treatment plan is essential for translating risk decisions into actionable, accountable steps. Therefore, the correct answer is a risk treatment plan.

QUESTION NO: 8
Scenario 3:
NovaCare is a US-based healthcare provider operating four hospitals and several outpatient clinics. Following several minor system outages and an internal assessment that revealed inconsistencies in security monitoring tools, top management recognized the need for a structured approach to identify and manage risks more effectively. Thus, they decided to implement a formal risk management process in line with ISO 31000 recommendations to enhance safety and improve resilience.
To address these issues, the Chief Risk Officer of NovaCare, Daniel, supported by a team of departmental representatives and risk coordinators, initiated a comprehensive risk management process. Initially, they carried out a thorough examination of the environment in which risks arise, defining the conditions under which potential issues would be assessed and managed.
Afterwards, Daniel and the team explored potential risks that could affect various departments. Using structured interviews and brainstorming workshops, they gathered potential risk events across departments.
Based on the scenario above, answer the following question:
In Scenario 3, what risk management activity did Daniel and the team conduct using structured interviews and brainstorming workshops?
A. Risk identification
B. Risk analysis
C. Risk evaluation
D. Risk treatment

Answer: A
Explanation:
The correct answer is A. Risk identification. ISO 31000:2018 defines risk identification as the process of finding, recognizing, and describing risks that could affect the achievement of objectives. Techniques such as structured interviews, brainstorming workshops, and expert consultations are explicitly recognized as appropriate methods for identifying risks.
In Scenario 3, Daniel and the team used structured interviews and brainstorming workshops to gather potential risk events across departments. This activity resulted in identifying key risks such as data breaches, record-keeping errors, and regulatory noncompliance. These outcomes clearly demonstrate risk identification rather than analysis or evaluation.
Risk analysis would involve understanding the nature of risks, including their causes, likelihood, and consequences. While the team later performed cause-and-effect analysis, the specific activity described in this question focuses on collecting and listing risk events, which is the core objective of risk identification.
From a PECB ISO 31000 Lead Risk Manager perspective, effective risk identification is critical for ensuring that significant risks are not overlooked and that subsequent analysis and treatment are meaningful. Therefore, the correct answer is risk identification.