적중율좋은ISO-31000-Lead-Risk-Manager높은통과율 시험대비자료덤프문제

참고: ITDumpsKR에서 Google Drive로 공유하는 무료, 최신 ISO-31000-Lead-Risk-Manager 시험 문제집이 있습니다: https://drive.google.com/open?id=1lSIbHeQdITpjqT1StZNtJksjkuy_mEcm

불과 1,2년전만 해도 PECB ISO-31000-Lead-Risk-Manager덤프를 결제하시면 수동으로 메일로 보내드리기에 공휴일에 결제하시면 덤프를 보내드릴수 없어 고객님께 페를 끼쳐드렸습니다. 하지만 지금은 시스템이 업그레이드되어 PECB ISO-31000-Lead-Risk-Manager덤프를 결제하시면 바로 사이트에서 다운받을수 있습니다. ITDumpsKR는 가면 갈수록 고객님께 편리를 드릴수 있도록 나날이 완벽해질것입니다.

PECB ISO-31000-Lead-Risk-Manager 시험요강:

주제	소개
주제 1	• Risk monitoring, review, communication, and consultation: Monitoring ensures effectiveness by tracking controls and identifying emerging risks. Communication engages stakeholders throughout all stages for informed decision-making.
주제 2	• Establishment of the risk management framework: The framework provides the foundation for implementing and improving risk management organization-wide. It encompasses leadership commitment, framework design, accountability, and resource allocation.
주제 3	• Fundamental principles and concepts of risk management: Risk management systematically identifies, analyzes, and responds to uncertainties affecting organizational objectives. Core principles include creating value, integration into processes, addressing uncertainty, and maintaining dynamic responsiveness.
주제 4	• Initiation of the risk management process and risk assessment: This domain establishes context and conducts systematic assessments to identify potential threats. Assessment involves identification, likelihood analysis, and prioritization against established criteria.

주제 5	• Risk treatment, risk recording and reporting: Treatment involves selecting measures to modify risks through avoidance, acceptance, removal, or sharing. Recording and reporting ensure systematic documentation and stakeholder communication.

최신 PECB ISO 31000 Certification ISO-31000-Lead-Risk-Manager 무료샘플문제 (Q75-Q80):

질문 # 75
What is one of the outputs of Business Impact Analysis (BIA)?

- A. Risk acceptance criteria
- B. Prioritized list of critical processes and their interdependencies
- C. Details of the organization's activities and resources
- D. Overview of the organization's business products and their relationship with processes

정답： B

설명：
The correct answer is A. Prioritized list of critical processes and their interdependencies. Business Impact Analysis (BIA) is a structured technique used to assess the consequences of disruptions to business activities and to identify which processes are critical to organizational objectives.
One of the key outputs of a BIA is the prioritization of critical processes, along with an understanding of their interdependencies, recovery time objectives, and potential impacts if disrupted. This information supports risk analysis, continuity planning, and resilience-building, all of which align with ISO 31000's emphasis on understanding consequences and supporting informed decision-making.
Option B may be an input to BIA but is not a primary output. Option C refers to general organizational descriptions rather than impact-focused analysis. Option D relates to risk evaluation, not BIA.
From a PECB ISO 31000 Lead Risk Manager perspective, BIA outputs are essential for prioritizing risks and allocating resources effectively. Therefore, the correct answer is a prioritized list of critical processes and their interdependencies.

질문 # 76
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:
Which risk treatment option did Trunroll use to address the risk of increasing dependence on third-party delivery platforms?

- A. Risk retention
- B. Risk avoidance
- C. Risk modification
- D. Risk sharing

정답：B

설명:
The correct answer is B. Risk avoidance. ISO 31000 defines risk treatment as selecting and implementing options for addressing risk, which may include avoiding the risk by deciding not to start or continue the activity that gives rise to the risk.
In Scenario 6, Trunroll explicitly decided not to move forward with planned partnerships with third-party delivery platforms. This decision was made after evaluating that the potential risks-loss of control over customer experience and sharply rising fees-outweighed the expected benefits. By choosing not to engage in these partnerships at all, Trunroll eliminated the source of the risk entirely.
This is a textbook example of risk avoidance, as described in ISO 31000 and reinforced in PECB ISO 31000 Lead Risk Manager training materials. Risk avoidance is appropriate when an activity poses unacceptable risk and alternative ways exist to meet objectives without engaging in that activity.
Risk modification would involve reducing likelihood or consequences while still engaging in the activity, which Trunroll did not do for delivery platforms. Risk sharing would involve transferring part of the risk to another party, such as through contracts or insurance, which also did not occur here. Risk retention applies when risks are knowingly accepted, which was not the case for this specific risk.
From a PECB ISO 31000 Lead Risk Manager perspective, avoiding the delivery platform partnerships was a deliberate, informed decision aligned with Trunroll's risk appetite and strategic objectives. Therefore, the correct answer is risk avoidance.

질문 # 77
Scenario 1:
Gospeed Ltd. is a trucking and logistics company headquartered in Birmingham, UK, specializing in domestic and EU road haulage. Operating a fleet of 25 trucks for both heavy loads and express deliveries, it provides transport services for packaged goods, textiles, iron, and steel. Recently, the company has faced challenges, including stricter EU regulations, customs delays, driver shortages, and supply chain disruptions. Most critically, limited and unreliable information has created uncertainty in anticipating delays, equipment failures, or regulatory changes, complicating decision-making.
To address these issues and strengthen resilience, Gospeed's top management decided to implement a risk management framework and apply a risk management process aligned with ISO 31000 guidelines. Considering the importance of stakeholders' perspectives when initiating the implementation of the risk management framework, top management brought together all relevant stakeholders to evaluate potential risks and ensure alignment of risk management efforts with the company's strategic objectives. The top management outlined the general level and types of risks it was prepared to take to pursue opportunities, while also clarifying which risks would not be acceptable under any circumstances. They accepted moderate financial risks, such as fuel price fluctuations or minor delays, but ruled out compromising safety or breaching regulations.
As part of the risk management process, the company moved from setting its overall direction to a closer examination of potential exposures, ensuring that identified risks were systematically analyzed, evaluated, and treated. Top management examined the main operational factors that significantly influence the likelihood and impact of risks. This analysis highlighted concerns related to supply chain disruptions, technological failures, and human errors.
Additionally, Gospeed's top management identified several external risks beyond their control, including interest rate changes, currency fluctuations, inflation trends, and new regulatory requirements. Consequently, top management agreed to adopt practical strategies to protect the company's financial stability and operations, including hedging against interest rate fluctuations, monitoring inflation, and ensuring compliance through staff training sessions.
However, other challenges emerged when top management pushed forward with a new contract for international deliveries without fully considering risk implications at the planning stage. Operational staff raised concerns about unreliable customs data and potential delays, but their input was overlooked in the rush to secure the deal. This resulted in delivery setbacks and financial penalties, revealing weaknesses in how risks were incorporated into day-to-day decision-making.
Based on the scenario above, answer the following question:

Which risk management principle did Gospeed's top management violate, resulting in delivery delays and financial penalties? Refer to Scenario 1.

- A. Continual improvement
- B. Integration
- C. Inclusive
- D. Dynamic

정답：C

설명：
The correct answer is B. Inclusive. ISO 31000:2018 identifies inclusiveness as a key principle of effective risk management. This principle requires appropriate and timely involvement of relevant stakeholders to ensure their knowledge, views, and perceptions are considered when managing risk. Inclusive risk management improves awareness, supports informed decision-making, and enhances ownership of risk responses.
In the scenario, Gospeed's top management failed to adequately consider input from operational staff when pursuing a new international delivery contract. Despite staff raising concerns about unreliable customs data and potential delays, their feedback was ignored in the rush to secure the deal. This directly contradicts the inclusiveness principle outlined in ISO 31000, which emphasizes that stakeholder engagement should occur at all stages of the risk management process, particularly when decisions have operational implications.
The consequence of this failure was delivery delays and financial penalties, demonstrating how excluding key stakeholders weakens risk identification, analysis, and treatment. While integration is also an important ISO 31000 principle, the issue described is not the absence of risk management from organizational processes, but rather the exclusion of relevant stakeholders from decision-making. Continual improvement relates to learning and enhancing the risk management framework over time, which is not the primary failure described. The dynamic principle concerns responding to change and emerging risks, whereas the core issue here was ignoring available knowledge.
From a PECB ISO 31000 Lead Risk Manager perspective, the scenario clearly illustrates a violation of the inclusive principle, making option B the correct answer.

질문 # 78
Scenario 5:
Crestview University is a well-known academic institution that recently launched a digital learning platform to support remote education. The platform integrates video lectures, interactive assessments, and student data management. After initial deployment, the risk management team identified several key risks, including unauthorized access to research data, system outages, and data privacy concerns.
To address these, the team discussed multiple risk treatment options. They considered limiting the platform's functionality, but this conflicted with the university's goals. Instead, they chose to partner with a reputable cybersecurity firm and purchase cyber insurance. They also planned to reduce the likelihood of system outages by upgrading server capacity and implementing redundant systems. Some risks, such as occasional minor software glitches, were retained after careful evaluation because they did not significantly affect Crestview's operations. The team considered these risks manageable and agreed to monitor and address them at a later stage. Thus, they documented the accepted risks and decided not to inform any stakeholder at this time.
Once the treatment options were selected, Crestview's risk management team developed a detailed risk treatment plan. They prioritized actions based on which processes carried the highest risk, ensuring cybersecurity measures were addressed first. The plan clearly defined the responsibilities of team members for approving and implementing treatments and identified the resources required, including budget and personnel. To maintain oversight, performance indicators and monitoring schedules were established, and regular progress updates were communicated to the university's top management.
Throughout the risk management process, all activities and decisions were thoroughly documented and communicated through formal channels. This ensured clear communication across departments, supported decision-making, enabled continuous improvement in risk management, and fostered transparency and accountability among stakeholders who manage and oversee risks. Special care was taken to communicate the results of the risk assessment, including any limitations in data or methods, the degree of uncertainty, and the level of confidence in findings. The reporting avoided overstating certainty and included quantifiable measures in appropriate, clearly defined units. Using standardized templates helped streamline documentation, while updates, such as changes to risk treatments, emerging risks, or shifting priorities, were routinely reflected in the system to keep the records current.
Based on the scenario above, answer the following question:
Based on Scenario 5, which step of the risk management process is reflected in the actions that promoted clear communication across departments, supported decision-making, enabled continuous improvement, and fostered accountability among stakeholders?

- A. Communication and consultation
- B. Monitoring and review
- C. Recording and reporting

- D. Risk evaluation

정답：C

설명：
The correct answer is A. Recording and reporting. ISO 31000:2018 emphasizes that recording and reporting are essential activities that support transparency, accountability, informed decision-making, and continual improvement in risk management. Recording ensures that information about risks, decisions, assumptions, and treatments is captured systematically, while reporting ensures that this information is communicated to appropriate stakeholders.
In Scenario 5, Crestview University ensured that all activities and decisions were thoroughly documented using standardized templates, that updates were reflected in the system, and that reports included limitations, uncertainty, and confidence levels. These characteristics align directly with the recording and reporting step of the risk management process. ISO 31000 explicitly states that recording and reporting should support governance, oversight, and continuous improvement.
Option B is incorrect because monitoring and review focus on tracking performance and changes over time, not primarily on documentation and communication. Option C is incorrect because communication and consultation emphasize engagement and dialogue with stakeholders rather than formal documentation. Option D is incorrect because risk evaluation compares analyzed risks against criteria.
From a PECB ISO 31000 Lead Risk Manager perspective, structured recording and reporting are critical to ensure traceability and learning. Therefore, the correct answer is recording and reporting.

질문 # 79
Scenario 5:
Crestview University is a well-known academic institution that recently launched a digital learning platform to support remote education. The platform integrates video lectures, interactive assessments, and student data management. After initial deployment, the risk management team identified several key risks, including unauthorized access to research data, system outages, and data privacy concerns.
To address these, the team discussed multiple risk treatment options. They considered limiting the platform's functionality, but this conflicted with the university's goals. Instead, they chose to partner with a reputable cybersecurity firm and purchase cyber insurance. They also planned to reduce the likelihood of system outages by upgrading server capacity and implementing redundant systems. Some risks, such as occasional minor software glitches, were retained after careful evaluation because they did not significantly affect Crestview's operations. The team considered these risks manageable and agreed to monitor and address them at a later stage. Thus, they documented the accepted risks and decided not to inform any stakeholder at this time.
Once the treatment options were selected, Crestview's risk management team developed a detailed risk treatment plan. They prioritized actions based on which processes carried the highest risk, ensuring cybersecurity measures were addressed first. The plan clearly defined the responsibilities of team members for approving and implementing treatments and identified the resources required, including budget and personnel. To maintain oversight, performance indicators and monitoring schedules were established, and regular progress updates were communicated to the university's top management.
Throughout the risk management process, all activities and decisions were thoroughly documented and communicated through formal channels. This ensured clear communication across departments, supported decision-making, enabled continuous improvement in risk management, and fostered transparency and accountability among stakeholders who manage and oversee risks. Special care was taken to communicate the results of the risk assessment, including any limitations in data or methods, the degree of uncertainty, and the level of confidence in findings. The reporting avoided overstating certainty and included quantifiable measures in appropriate, clearly defined units. Using standardized templates helped streamline documentation, while updates, such as changes to risk treatments, emerging risks, or shifting priorities, were routinely reflected in the system to keep the records current.
Based on the scenario above, answer the following question:
The risk management team of Crestview documented the accepted risks and decided not to inform any stakeholder at this time. Is this acceptable?

- A. No, accepted risks must always be eliminated
- B. Yes, as long as the risks are removed from the risk register after they have been addressed
- C. Yes, once risks are documented, there is no need to inform stakeholders until the risks become critical
- D. No, when the risk is accepted, the stakeholders must be informed to accept the risk

정답：D

설명：
The correct answer is C. No, when the risk is accepted, the stakeholders must be informed to accept the risk. ISO 31000 requires that risk acceptance decisions are made transparently and with appropriate authority. Risk acceptance is not merely a technical decision; it is a governance decision that must involve or be communicated to relevant stakeholders.
In Scenario 5, Crestview University documented accepted risks but chose not to inform stakeholders. While documentation is

necessary, ISO 31000 emphasizes that communication and consultation should occur throughout the risk management process, including when risks are accepted. Stakeholders with accountability or oversight responsibilities must be aware of accepted risks so they can consciously agree to them and understand their implications.
Option A is incorrect because withholding information undermines transparency and accountability. Option B is incorrect because accepted risks typically remain in the risk register for monitoring, not removal. Option D is incorrect because ISO 31000 recognizes that not all risks can or should be eliminated.
From a PECB ISO 31000 Lead Risk Manager perspective, risk acceptance requires informed consent by authorized stakeholders. Therefore, the correct answer is no, stakeholders must be informed when risks are accepted.

질문 # 80
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, fraserqbzi650994.activoblog.com, www.stes.tyc.edu.tw, thebookmarkking.com, dawudcouo234523.blogdomago.com, animationeasy.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

참고: ITDumpsKR에서 Google Drive로 공유하는 무료 2026 PECB ISO-31000-Lead-Risk-Manager 시험 문제집이 있습니다: https://drive.google.com/open?id=1lSIbHeQdITpjqT1StZNtJksjkuy_mEcm