As part of the methodology development process for the 2024 CSA, we kindly invite you to review a draft proposal for new and updated questions impacting your industry.

Please review this document and provide your feedback by completing the online survey.

The question texts and methodology presented may be subject to change at any time before the end of March 2024. In addition, questions may look different in the Online Assessment Tool in terms of question structure and layout.
Introduction

Criterion Rationale

Effective risk and crisis management is vital for long-term financial planning and organizational flexibility. Since the financial crisis, it has gained particular importance. Companies need to implement internal control processes to comply with existing regulations and proactively develop control mechanisms. These questions focus on risk governance, the frequency of risk reviews, emerging risks, incentivizing, training and empowering employees in order to develop an effective risk culture. Additionally, we perform a real-time check to assess the system with our internal MSA (Media and Stakeholder Analysis). The scope of the criterion may vary depending on a company’s size and ownership structure.

Reason for update and summary of changes

As the world continues to face unexpected events such as geopolitical conflicts with material repercussions on corporations, investors are looking for solid risk management processes to ensure that organizations are equipped to sustain impacts on business performance. This document contains the proposed changes to the existing questions “Risk Governance”, “Risk Management Processes” and “Risk Management” (for non-listed companies) to reflect best practices such as the implementation of the three lines of defense model as a risk governance framework. While the question “Risk Culture” has been removed, relevant aspects have been retained and integrated in the questions “Risk Management Processes” and “Risk Management”. Please note that in the following sections, new content added to the questions has been framed in red.

To implement the changes described above, some minor changes have been applied to the wording of all three questions.
Updated Question

**Question: Risk Governance**

**INDUSTRIES IMPACTED:**

All Industries

**QUESTION RATIONALE**

The purpose of this question is to assess the effectiveness of a company's risk management procedures. For this, it is important that the company's senior management and board of directors are not just aware of risks but also actively involved in managing them. While the board of directors is ultimately responsible for risk management, it is up to the senior management to take the board's strategic direction and turn it into appropriate policies and procedures, as well as effectively implement, execute, and monitor these policies.

The “three lines of defense model” is a recognized governance framework for managing risks. It lays out clear risk management responsibilities and accountabilities to ensure that a company’s risk-related objectives are achieved. In this model, the first and second lines are responsible for executing and monitoring risk management activities. The third line, on the other hand, operates independently to check how well the risk management processes are working.

**KEY DEFINITIONS**

**Board Level Risk Oversight**

*Board level responsibility:* a dedicated role or committee at the highest governing body consisting of independent and/or non-executive Board member(s). This could be a Risk Committee, or an Audit Committee tasked with explicit responsibility for risk management overview.

**Operational Management Functions (Three Lines of Defense Model)**

*Operational Risk Ownership (first line):* the employees or teams directly involved in producing and/or delivering products and services to clients. They are responsible for owning and managing risks in the day-to-day operations. The first line is responsible for the execution of controls set by the second line. We expect clear assignment of risk management responsibilities at the business unit level, which could include roles such as Risk Owners, Risk Managers and Business Unit Heads.

*Risk Management and Compliance Oversight (second line):* the individual, committee or body in the organization that is charged with monitoring and supporting risk management processes, ensuring
that risk management objectives are achieved. This oversight typically falls under senior management or the executive level, responsible for setting control standards and overseeing compliance. Examples of responsible people or committees include the Chief Risk Officer, Risk Management Committee and Chief Compliance Officer. Note: Given that the CEO has ultimate responsibility for all aspects of a company’s operations, the CEO is not accepted here, but rather the expected function would report to senior management or the CEO.

**Independent Audit Unit (third line):** the unit tasked with advising and auditing to ensure policies are followed and processes are executed in line with management’s selected performance goals and risk tolerances. This could be an internal audit or a comparable external function, providing an independent assurance that organizational practices are aligned with the company’s risk strategy and policies, as implemented by the first and second lines. The independence of this unit ensures objective monitoring and control of various risks, safeguarding the organization’s interests without conflicts of interest arising from other business priorities. This function typically reports directly to the board of directors on top of senior/executive management and remains separate from the implementation of processes or risk management to preserve its objectivity. Note: The responsibilities of internal audit as part of the third line of defense extend beyond financial reporting compliance audits.

**DATA REQUIREMENTS**

- The document(s) you attached will be used to verify your response. The supporting documents need to be available in the public domain (e.g., annual report, sustainability report, integrated report, company publications) or corporate website.
- Any response that cannot be verified in the attached document(s) will not be accepted.

**REFERENCES**

- COSO Framework
- The Institute of Internal Auditors

**QUESTION LAYOUT**

Previous layout:
The question requires publicly available information.

Please indicate which people, departments and committees are responsible and accountable for enterprise risk management in terms of risk appetite & tolerance as well as risk monitoring & reporting. Please also indicate the expertise and training applicable to non-executive directors as well as the corporate structure of risk management functions. Please indicate where this information is available in your public reporting.

- Yes, our company has people, departments and committees that are responsible and accountable for enterprise risk management in terms of risk appetite & tolerance as well as risk monitoring & reporting and are available in the public reporting.

<table>
<thead>
<tr>
<th>Highest ranking person with dedicated risk management responsibility on an operational level (not CEO)</th>
<th>Please indicate name and position</th>
<th>Reporting line: please indicate who the person or committee reports to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest ranking person with responsibility for monitoring and auditing risk management performance on an operational level (not CEO)</td>
<td>Dropout:</td>
<td>Dropout:</td>
</tr>
<tr>
<td></td>
<td>Max: 1000 chars</td>
<td>Max: 1000 chars</td>
</tr>
<tr>
<td></td>
<td>Chief Risk Officer or Risk Committee</td>
<td>Executive Management</td>
</tr>
<tr>
<td></td>
<td>Other person on committee</td>
<td>Board of Directors</td>
</tr>
<tr>
<td></td>
<td>No information available</td>
<td>Other reporting line</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No information available</td>
</tr>
</tbody>
</table>

- Number of non-executive members of board of directors/supervisory board with expertise in (enterprise) risk management. Please specify number of non-executive directors and provide supporting evidence.

- Regular risk management education for non-executive directors ensured. Please specify and provide supporting evidence.

- The risk management function is structurally independent of the business lines. Please specify and provide supporting evidence.

- No, there are no such responsibilities in place.
  - Not applicable. Please provide an explanation in the comment box below.
*The question requires publicly available information.

Does your company have a risk governance framework in place? Please provide supporting evidence for all the options selected and indicate where this is available in your public reporting or corporate website.

- Yes, we publicly disclose our risk governance framework

We have a risk governance framework with board level risk oversight:

- Dedicated role or committee at board level for risk oversight (independent and/ or non-executive Board member(s))

We have a risk governance framework with dedicated operational risk management functions in place:

- Operational Risk Ownership (first line): front-line employees or dedicated operational roles (e.g., Risk Managers, Business Unit Heads) own and manage risks.

- Risk Management and Compliance Oversight (second line): a dedicated role or committee exists at the senior management or executive level, which is responsible for setting control standards and oversees compliance with them. (Does not include the CEO).

- Independent Audit Unit (third line): an internal audit function that provides independent assurance on the effectiveness of risk management and compliance processes.

- No, we do not publicly report this information.
- Not applicable. Please provide an explanation in the comment box below.
Updated Question

**Question: Risk Management Processes**

**INDUSTRIES IMPACTED:**

All industries

**QUESTION RATIONALE**

The purpose of this question is to assess a company’s risk management practices and strategies, essential for fostering an effective risk culture. Effective risk and crisis management are vital for long-term financial stability and adaptability. Implementing internal control processes ensures compliance with current regulations and positions a company to proactively refine these controls.

Conducting robust risk assessments, including evaluating risk exposure and determining risk appetite, allows companies to respond strategically to events that may have a material impact. Moreover, regular and frequent risk reviews and audits can further enhance the effectiveness of risk management processes. To embed these practices into the wider organization, measures should be taken to educate and incentivize employees at all levels of the business, thereby nurturing a strong and effective risk culture. Such an approach ensures that risk management is not just a compliance exercise but a fundamental part of the company's operational mindset.

**KEY DEFINITIONS**

To answer this question, it is important to focus on the organization’s general approach to risk identification and risk review, rather than specific areas such as Occupational Health & Safety, Human Rights or Climate Change. Reports like those from the Task Force on Climate-related Financial Disclosures (TCFD) or the Carbon Disclosure Project (CDP) are not considered suitable evidence in this context. However, if Climate Change is identified as a significant material risk, we would expect it to be reported in the overarching risk section.

**Risk review**

A risk review is a process that involves identifying risks and assessing or reassessing their impact and likelihood. This process includes updating the status of various risks and implementing procedures to identify hazards, determine potential negative effects, and minimize or eliminate risks.

The elements that define a risk review and are considered best practice include:

- **Description of the company specific risk exposure:** this should at least evaluate the potential magnitude and likelihood of the risk, considering the factors unique to the
business or industry in order to define the impact of the risk on the company. We expect risk exposure to be reported for at least two of the identified risks.

- **Process or framework to determine risk appetite**: there should be a clearly defined process or framework outlining how the risk appetite (the level of risk the company is willing to take) is set for the identified risks, including who within the organization is responsible for this.
- **Description of mitigating actions**: actions taken to reduce the severity of the risk and the likelihood of potential negative impacts should be described. We expect mitigating actions to be reported alongside at least two of the identified risks.

**Review of risk exposure**

Regular reviews are essential to keep up with changes in the risk landscape that could affect the company's risk exposure. These reviews help the organization stay resilient against potential risks. They ensure that the designated risk appetite and mitigating actions stay up-to-date and relevant. The mere reporting of risk exposure indicators in e.g., the annual report is not considered sufficient evidence of an active risk exposure review process.

**Audit of risk management in the last two years**

This involves a systematic assessment of the methods, tools and processes used in identifying, evaluating, controlling, monitoring, and reporting risks. Per best practice, audits can be conducted by qualified, internal auditors and by qualified, independent third-party auditors. These audits should follow guidelines on management systems audits or risk management standards like ISO 31000 and should be conducted at least every two years. Audits related to internal control of financial reporting are not considered sufficient here.

**Promotion of an effective risk culture**

Creating a strong risk culture is important for integrating risk processes, procedures and employee awareness throughout the organization. This can be achieved by offering financial incentives tied to meeting risk-related goals, providing training and education to all employees, and considering risk factors when developing new products or services.

**DATA REQUIREMENTS**

- The document(s) you attached will be used to verify your response. The supporting documents need to be available in the public domain (e.g., annual report, sustainability report, integrated report, company publications) or corporate website.
- Any response that cannot be verified in the attached document(s) will not be accepted.

**REFERENCES**

COSO Framework

ISO 31000:2018 Risk Management
**Does your company have risk management processes in place? Please provide supporting evidence for the options selected and for the first aspect please indicate where this is available in your public reporting or corporate website.**

- Yes, our company has risk management processes in place

### Risk Review
- We publicly report on risks identified including a description of the risk, its likelihood and magnitude of the potential impact.
- The process includes the following elements:
  - Description of risk appetite or risk tolerance levels for at least two risk categories/types
  - Prioritization of identified risks
  - Description of mitigating actions for at least 2 identified risks

### Sensitivity Analysis and Stress testing
- We perform sensitivity analysis or stress testing on financial risks and/or non-financial risks:
  - Sensitivity analysis or stress testing on financial risks
  - Sensitivity analysis or stress testing on non-financial risks

### Review of company’s risk exposure on a regular basis
- We review our company’s risk exposure on a regular basis. Please attach evidence of the frequency of the assessments.
  - At least twice a year or more frequently
  - At least yearly
  - Less frequently or not specified

### Audit of the risk management process in the last two years
- We conduct an audit of the risk management process. Please specify if an internal audit and/or an external audit have been performed and provide supporting evidence if multiple choice.
  - Yes, we have conducted an internal audit
  - Yes, we have conducted an external audit

- No, we do not publicly report on our risk management processes.
- Not applicable. Please provide a comment below
The question requires publicly available information.

Does your company have risk management processes in place? Please provide supporting evidence for all the options selected and please indicate where this is available in your public reporting or corporate website.

- Yes, we publicly report on the following aspects of our risk management processes:

  Our risk review process includes the following aspects:

  - Description of the company specific risk exposure (considering likelihood and magnitude) of at least 2 identified risks
  - Description of process or framework to determine the risk appetite for identified risks
  - Description of mitigating actions for at least 2 identified risks

  We review our company’s risk exposure on a regular basis. Please attach evidence of the frequency of the assessments:

  - At least twice a year or more frequently
  - At least yearly
  - Less frequently than yearly
  - Not specified

  We have conducted an audit of the risk management process. Please specify if an internal audit and/or an external audit have been performed.

  - Yes, we have conducted an internal audit in the last two years
  - Yes, we have conducted an external audit in the last two years

  We have strategies in place to promote an effective risk culture throughout the organisation:

  - Regular risk management education for non-executive directors
  - Focused training throughout the organization on risk management principles
  - Incorporation of risk criteria in the development of products and services
  - Financial incentives which incorporate risk management metrics

  - No, we do not publicly disclose this information.
  - Not applicable. Please provide an explanation in the comment box below.
Updated Question

**Question: Risk Management**

**INDUSTRIES IMPACTED:**

All industries (non-listed companies only)

**QUESTION RATIONALE**

The purpose of this question is to obtain a better understanding of a company's risk governance and risk review practices which are critical for overall risk control and mitigation. For a company's risk management procedures to be most effective, risk awareness concerns and management must be overseen by a company's senior leadership or board of directors. Moreover, frequent risk reviews, the structural independence of the risk management functions as well as regular audits can further improve risk management procedures and effectiveness.

**KEY DEFINITIONS**

**Risk review:** a risk review can constitute an assessment or re-assessment of a certain risk exposure, a status update thereof, a sensitivity analysis with regards to a certain risk or other procedures and processes that aim to identify hazards, determine potential negative effects, and ultimately remove or minimize a certain risk. A risk review should include the following aspects:

- A description of how the risk affects the organization (E.g., Revenues, profitability, costs)
- The likelihood of impact on the organization,
- The magnitude of the potential business impact,
- Mitigation actions,
- The frequency of review

**Examples of risks** considered in this question:


**Board level responsibility:** a dedicated committee at the highest governing body, i.e., Risk Committee or Audit Committee with explicit risk management overview tasks.

**Executive level responsibility:** a dedicated function at the executive level (C-Suite), e.g., Chief Risk Officer.
Responsibility at business unit level: dedicated risk management functions below the executive level, e.g., Risk managers.

Reporting Line: under reporting line, the whole reporting line from the responsible persons or committee up to the executive managers or board of directors should be considered.

Structural independence: this means that the organization’s risk function is independent of other business functions, departments, or divisions, and serves as a means to address risks throughout the entire organization and not just within a specific department (for example, if the risk management function is a separate reporting pillar altogether or reports directly to the CEO). Structural independence allows for objective monitoring and control of various risks, in the best interest of the entire organization and without the pressure of a potential conflict of interest coming from other business priorities.

Audit of risk management: systematically assesses the measures, tools, and processes applied to identifying, evaluating, controlling, monitoring, and reporting on relevant risks to the organization, considering their likelihood and potential of impact. It can be realized by qualified, internal auditors or by qualified, independent third-party auditors, following good practice guidelines on management systems audits or risk management guidelines such as ISO 31000.

Promotion of an effective risk culture: a strong risk culture is important to embed risk processes, procedures, and employee awareness into the overall organization. This could be through providing financial incentives linked to the attainment of risk related targets or criteria, training, and education for all employees up to board level and incorporating risk criteria during the development of new products or services.

DATA REQUIREMENTS

- The document(s) you attached will be used to verify the qualitative part of your response. If a question text field is available, a comprehensive answer in that field can be accepted instead of a supporting document. Any qualitative response that cannot be verified in the attached document(s) will not be accepted.
- The supporting documents do not need to be available in the public domain.

REFERENCES

COSO Framework

ISO 31000:2018 Risk Management
**QUESTION LAYOUT**

Does your company have any documented risk management procedures and positions in place?
  - Yes, our company has risk management procedures and positions in place.

<table>
<thead>
<tr>
<th><strong>Review of company's risk exposure on a regular basis</strong></th>
<th>We formally review our company’s risk exposure on a regular basis for at least two types of risks. Please attach your latest risk review(s) and evidence of the frequency of the assessments:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>o At least twice a year or more frequently</td>
</tr>
<tr>
<td></td>
<td>o At least yearly</td>
</tr>
<tr>
<td></td>
<td>o Less frequently than yearly</td>
</tr>
<tr>
<td></td>
<td>o Not specified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Oversight of company's risk exposure</strong></th>
<th>We have dedicated risk management functions in place. Please indicate the highest level at which your company overviews the risk exposure and provide supporting evidence for the respective role or committee:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>o Dedicated role or committee at board level</td>
</tr>
<tr>
<td></td>
<td>o Dedicated role or committee at executive level</td>
</tr>
<tr>
<td></td>
<td>o Dedicated role(s) at business unit level</td>
</tr>
<tr>
<td></td>
<td>o Not specified</td>
</tr>
</tbody>
</table>

| **Structural Independence** | ☐ The risk management function is structurally independent from the business lines. Please specify and provide supporting evidence (E.g., Org chart of reporting lines): |

<table>
<thead>
<tr>
<th><strong>Audit of the risk management process in the last two years</strong></th>
<th>We have conducted an audit of the risk management process in the last two years. Please specify if an internal audit, external audit or both have been performed and provide supporting evidence.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>☐ Yes, we have conducted an internal audit in the last two years</td>
</tr>
<tr>
<td></td>
<td>☐ Yes, we have conducted an external audit in the last two years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Risk Culture</strong></th>
<th>We have strategies in place to promote an effective risk culture throughout the organisation:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>☐ Regular risk management education for non-executive directors</td>
</tr>
</tbody>
</table>
- Focused training throughout the organization on risk management principles
- Incorporation of risk criteria in the development of products and services
- Financial incentives which incorporate risk management metrics

- No, we do not have any documented risk management procedures or positions in place.
- Not applicable. Please provide a comment below.
- Not known
Contact Us

CSA Helpline
+41 44 529 5160

Copyright © 2024 S&P Global Inc. All rights reserved.

Unless otherwise noted, all information, data and other material, including ratings or scores (all such information, “Content”) contained in this publication and other reports, materials, or websites of S&P Global Inc. and/or its affiliates is the exclusive property of S&P Global (Switzerland) SA, a subsidiary of S&P Global Inc., and/or its relevant affiliates (individually and collectively “S&P”) and may not be copied or reproduced in any form except with the prior written permission of S&P. The Content shall not be used for any unlawful or unauthorized purposes. This publication is derived from sources believed to be accurate and reliable, but it is each reader’s responsibility to evaluate the accuracy, completeness and usefulness of any opinions, statements or other Content contained in this publication. The Content and any other material and information in this publication are provided “as is” and without warranties of any kind, either expressed or implied. S&P Global (Switzerland) SA, a subsidiary of S&P Global Inc., and/or its relevant affiliates disclaim all warranties, expressed or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose.

S&P (and any third-party providers, as well as their directors, officers, shareholders, employees or agents) does not guarantee the accuracy, adequacy, completeness, timeliness or availability of any Content and are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of such Content. In no event shall S&P (and any third-party providers, as well as their directors, officers, shareholders, employees or agents) be liable for any direct, indirect, special, incidental, and/or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profit and opportunity costs) in connection with any use of the Content (including, without limitation, any opinions or other information expressly or implicitly contained in this publication).

Any opinions and views in this publication reflect the current judgment of the authors and may change without notice. Further, any opinions and views expressed by CSA participants do not reflect the policies or positions of S&P or any other person, organization or company. The Content contained in this publication is distributed with the understanding that the authors, publishers and distributors are not rendering legal, accounting or other professional advice or opinions on specific facts or matters and accordingly assume no liability whatsoever in connection with its use. The Content contained in this publication constitutes neither a solicitation, nor a recommendation, nor an offer to buy or sell investment instruments or others services, or to engage in any other kind of transaction, and such information is not directed to persons in any jurisdiction where the provision of such Content would run counter to local laws and regulations. S&P keeps certain activities of its business units separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain business units of S&P may have information that is not available to other S&P business units. S&P has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.


S&P Global Switzerland AG, Zurich Branch, Neumuehlequai 6, 8001 Zurich, Switzerland