METHODOLOGY FEEDBACK REQUEST CSA 2027

Risk & Crisis Management

DEADLINE FOR FEEDBACK:

27th November 2026

As part of the methodology development process for the 2027 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 2027. 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 are vital for long-term value creation and business continuity. As we navigate an increasingly complex and interconnected world, the ability to identify, assess, and manage risks has become more important than ever. Companies are expected to implement internal control processes to manage these risks and comply with applicable regulations. This criterion focuses on risk governance, the processes for managing risks and risk identification. These questions apply to all companies. Banks and Financial companies are assessed on additional elements related to industry-specific regulations.

Reason for update and summary of changes

This document contains proposals under the Risk & Crisis Management

The “Emerging Risks” question, now referred to as “Risk Identification,” has been updated to focus on the identification and quality of reporting rather than on the content of individual risks. Additionally, the risk identification from the “Risk Management Process” question has been moved over. In this way, the structure of the criterion has been clarified, so that governance, management, and identification are assessed separately. The requirements for risk identification have been lessened to allow for any risk. However, more credit is granted to companies that can demonstrate long-term risk management. The individual requirements are no longer bundled, allowing for a more nuanced and flexible assessment.

Updated Question

Question: Risk Management Process

INDUSTRIES IMPACTED:

All industries (62)

QUESTION RATIONALE

This question assesses 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 for a company to refine these controls proactively.

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 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 risk management is not just a compliance exercise but a fundamental part of the company's operational mindset.

KEY DEFINITIONS

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 to stay resilient against potential risks. They ensure that the designated risk appetite and mitigating actions remain up to date and relevant. The mere reporting of risk exposure indicators, e.g., in the annual report, is not considered sufficient evidence of an active risk exposure review process.

Audit of risk management processes in the last two years: This involves a systematic assessment of the methods, tools and processes used to identify, evaluate, control, monitor, and report risks. Per best practice, audits can be conducted by qualified internal auditors and qualified independent third-party auditors. These audits should follow guidelines for management systems audits or risk management standards, such as ISO 31000, and should be conducted at least every two years.

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:

- **Regular risk management education for non-executive directors:** Education of board members should be recurring and specific to risk management. This is different from regular risk reporting to the board.
- **Providing training to all employees:** Training must cover risk management and be provided at a group level.

- **Considering risk factors when developing new products or services:** Risk criteria can be linked to financial risks, regulatory risks, operational risks, etc.
- **Offering financial incentives tied to meeting risk-related goals:** Incentives should be related to specific risks the company has identified as key concerns. For instance, if health and safety is identified as the primary risk, the incentives should be directly linked to this risk and initiatives to reduce associated health and safety risks.
- **Risk appetite:** The process of defining, or the resulting level of, risk that a company is willing to accept in pursuit of its objectives.

DATA REQUIREMENTS

To answer this question, it is important to focus on the organization's general approach to risk identification and review, rather than on specific areas such as occupational health & safety, human rights, biodiversity, or climate change. Reports such as those aligned with IFRS S2 from the International Sustainability Standards Board (ISSB), the Task Force on Climate-related Financial Disclosures (TCFD), or the Carbon Disclosure Project (CDP) are not considered suitable evidence in this context.

Audit

- Please provide information about the audits conducted on your risk management processes in the last two years
- The frequency should be clearly reported

Not acceptable for 'The company has conducted an audit of the risk management process':

- A policy or commitment to conduct audits every two years
- Audits related to internal controls of financial reporting
- Audit of the financial statements

Risk Culture

Not acceptable for 'board of directors training on how to manage risks':

- Directors' induction or orientation programs that cover risk management, as these are typically one-off events rather than ongoing education.
- Training that is solely about specific topics, such as new regulations or policies.
- Trainings are only provided to selected directors, implying that not all non-executive directors receive these trainings.
- If non-executive directors are "encouraged" or "guided" or "recommended" to take training. Instead, please provide specific evidence that education is provided or mandated.
- The board receives briefings or reports from committees.

- If the board is updated on internal risk management matters, as this is a mere reporting on risk management performance to the board of directors and is not equivalent to a formal training or education.

Not acceptable for 'focused training throughout the organization on risk management principles':

- Information for trainings which are focused on specific topics such as new regulations, policies, health and safety, or cybersecurity is not accepted as these are considered trainings on specific risks, not overall risk management.

Risk Appetite

- The process described for identifying the risk appetite or
- A description of the risk appetite generally or as part of a specific risk

REFERENCES

COSO Framework

ISO 31000:2018 Risk Management

QUESTION LAYOUT

Notice: The question requires publicly available information.

Does the company have risk management processes to promote an effective risk culture?
Listed companies are required to provide links to public reports or corporate websites.
Non-listed companies are required to provide internal documents and/or links to public reports or corporate websites.

- ○ Yes, the company has risk management processes to promote an effective risk culture.

  Max. 3 public references

The risk review process include the following elements:

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

The company reviews its risk exposure regularly:

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

The company has conducted an audit of the risk management process. Please specify if an internal audit and/or an external audit has been performed:

- ☐ Yes, the company has conducted an internal audit in the last two years
- ☐ Yes, the company has conducted an external audit in the last two years

The company has strategies in place to promote an effective risk culture throughout the organization:

- ☐ Regular risk management education for all 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 that incorporate risk management metrics
- ☐ The risk appetite has been defined

- ○ No, the company does not have risk management processes to promote an effective risk culture.
- ○ The question is not applicable to the company.

Updated Question

Question: Risk Identification (formerly Emerging Risks)

INDUSTRIES IMPACTED:

All industries (62)

QUESTION RATIONALE

It is important for companies to identify and clearly disclose their risks, including their nature, characteristics, potential impacts, likelihood, and mitigation actions. Effective risk disclosure enables stakeholders to understand the uncertainties that may affect the company's strategy, operations, financial performance, reputation, and long-term sustainability.

Transparent disclosure supports informed decision-making and strengthens stakeholder confidence. It demonstrates that the company acknowledges the risks associated with its activities and is actively managing them rather than concealing or minimizing them. The quality of a company's risk descriptions also indicates the maturity of its risk management process. This level of clarity generally reflects that risks have been properly identified, assessed, prioritized, owned, and monitored within the organization.

KEY DEFINITIONS

Company-specific description: A clear statement of the potential event or condition, and how that could affect the company specifically.

Categories: The classification assigned to the respective risk based on its nature.

Likelihood: The estimated probability that the risk event will occur within the defined timeframe.

Magnitude: The estimated severity of the consequences if the risk occurs, considering factors such as financial loss, operational disruption, regulatory impact, reputational damage, or effects on customers and employees.

Mitigating action: A measure taken or planned to reduce the likelihood of the risk occurring, limit its impact, or improve the company's ability to respond.

Timeframe: The period in which the risk is expected to arise, become more likely, produce an impact, or require action.

DATA REQUIREMENTS

To answer this question, it is important to focus on the organization's general approach to risk identification and review, rather than on specific areas such as occupational health & safety, human rights, biodiversity, or climate change. Reports such as those aligned with IFRS S2 from the International Sustainability Standards

Board (ISSB), the Task Force on Climate-related Financial Disclosures (TCFD), or the Carbon Disclosure Project (CDP) are not considered suitable evidence in this context.

Company-specific description:

- The description of the event or condition can be generic, but the impact must be specific to the company. It can be linked to the company as a whole or to a specific aspect, such as a product or asset.
- Generic risk or impact descriptions that can be applied to other companies are not acceptable.

Categories:

- The risks should be aligned with one of the categories on the list
- If several categories can be selected, the most relevant category should be selected
- Categories not on the list, usually business-specific, will not be accepted. See the list of unacceptable risks below for more information.

Likelihood:

- Likelihood may be expressed using a scale such as rare, unlikely, possible, likely, or almost certain.
- Risks for which an impact has already occurred and are likely to occur again are also acceptable.
- Hypothetical generic language is not acceptable. That is, for example, when the risk is described as "may" or "could" occur.

Magnitude:

- The severity of the impact on the relevant aspect of the company should be described.
- The impact can be described qualitatively by, for example, using terms such as "significant," "material" and "substantial," or it can be quantified.
- Reference to specific aspects such as loss of revenues, increased cost or harm to the environment/people is also acceptable.

Mitigating action:

- The actions must be specific to addressing the risk or impact.
- It can be planned or already in execution.
- Completed actions will also be accepted if the risk is still impacting or the impact is only expected in the future.

Timeframe:

- The timeframe should describe the estimated timing and, where relevant, duration of the risk's impact.
- Qualitative descriptions or ranges are allowed in cases where the timing is uncertain.
- It can be described as an actual timeline, or indirectly, with terms such as short-term and long-term.

Not acceptable risks

- Litigation risk
- Regulatory risk (except if it is linked to a specific future regulation that is uncertain and can have an impact that requires the company to change its strategy. This new regulation needs to be linked to an external risk.)
- Commodity risk or price risk
- Competition/market risk (Risks mentioning the impact on the competitive landscape based on technological or societal developments are acceptable)
- Operational risk, such as IT failures, data breaches, and cybersecurity breaches. If cybersecurity and data privacy are mentioned in relation to a new technological development, such as the Internet of Things (IoT), Artificial Intelligence (AI), or Bioengineering, they can be accepted.
- Potential mergers and acquisitions within its market
- Currency risk
- Climate change and biodiversity risks (assessed separately)

REFERENCES

World Economic Forum – The Global Risks Report

QUESTION LAYOUT

Notice: The question requires publicly available information.

Does the company report on long-term, emerging risks?
Listed companies are required to provide links to public reports or corporate websites.
Non-listed companies are required to provide internal documents and/or links to public reports or corporate websites.

- ○ Yes, the company reports on long-term emerging risks.

Aspects	Emerging risk 1	Emerging risk 2
Supporting evidence	Max. 3 public references	Max. 3 public references
Name of the emerging risk	Text box	Text box
Category	Drop-down menu	Drop-down menu
Description	☐ The company reports on the description and specification of emerging risk 1 in the context of its business. Please provide the description in the text box below. Text box	☐ The company reports on the description and specification of emerging risk 2 in the context of its business. Please provide the description in the text box below. Text box
Impact	☐ The company reports on the potential impact of emerging risk 1 on its business. Please provide the impact description in the text box below. Text box	☐ The company reports on the potential impact of emerging risk 2 on its business. Please provide the impact description in the text box below. Text box
Mitigating actions	☐ The company reports on the mitigating actions of emerging risk 1. Please provide the description of the mitigating actions in the text box below. Text box	☐ The company reports on the mitigating actions of emerging risk 2. Please provide the description of the mitigating actions in the text box below. Text box

- ○ No, the company does not report on long-term emerging risks.
- ○ The question is not applicable to the company.
- ○ The information is not available.

Does the company report on the risks identified?
Listed companies are required to provide links to public reports or corporate websites.
Non-listed companies are required to provide internal documents and/or links to public reports or corporate websites.

- ○ Yes, the company reports on the risks identified. Please indicate where this information is available in **public reporting or corporate website.**

Max. 5 public references

Aspects	**Description**	**Characteristics**
Risk 1	☐ Company-specific description Category Drop-down menu	☐ Likelihood ☐ Magnitude ☐ Mitigating action ☐ Timeframe
Risk 2	☐ Company-specific description Category Drop-down menu	☐ Likelihood ☐ Magnitude ☐ Mitigating action ☐ Timeframe

- ○ No, the company does not publicly report on risks identified.
- ○ The question is not applicable to the company.

Contact Us

CSA Helpline
+41 44 529 5160

Copyright© 2026 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.

For information provided as part of the CSA questionnaire refer to our "Use of Information and Confidentiality Policy" https://portal.s1.spglobal.com/survey/documents/Use_of_Information_Policy.pdf and for personal information provided to S&P refer to S&P Global's Privacy Policy: https://www.spglobal.com/en/privacy/privacy-policy-english.

S&P Global Switzerland AG, Zurich Branch