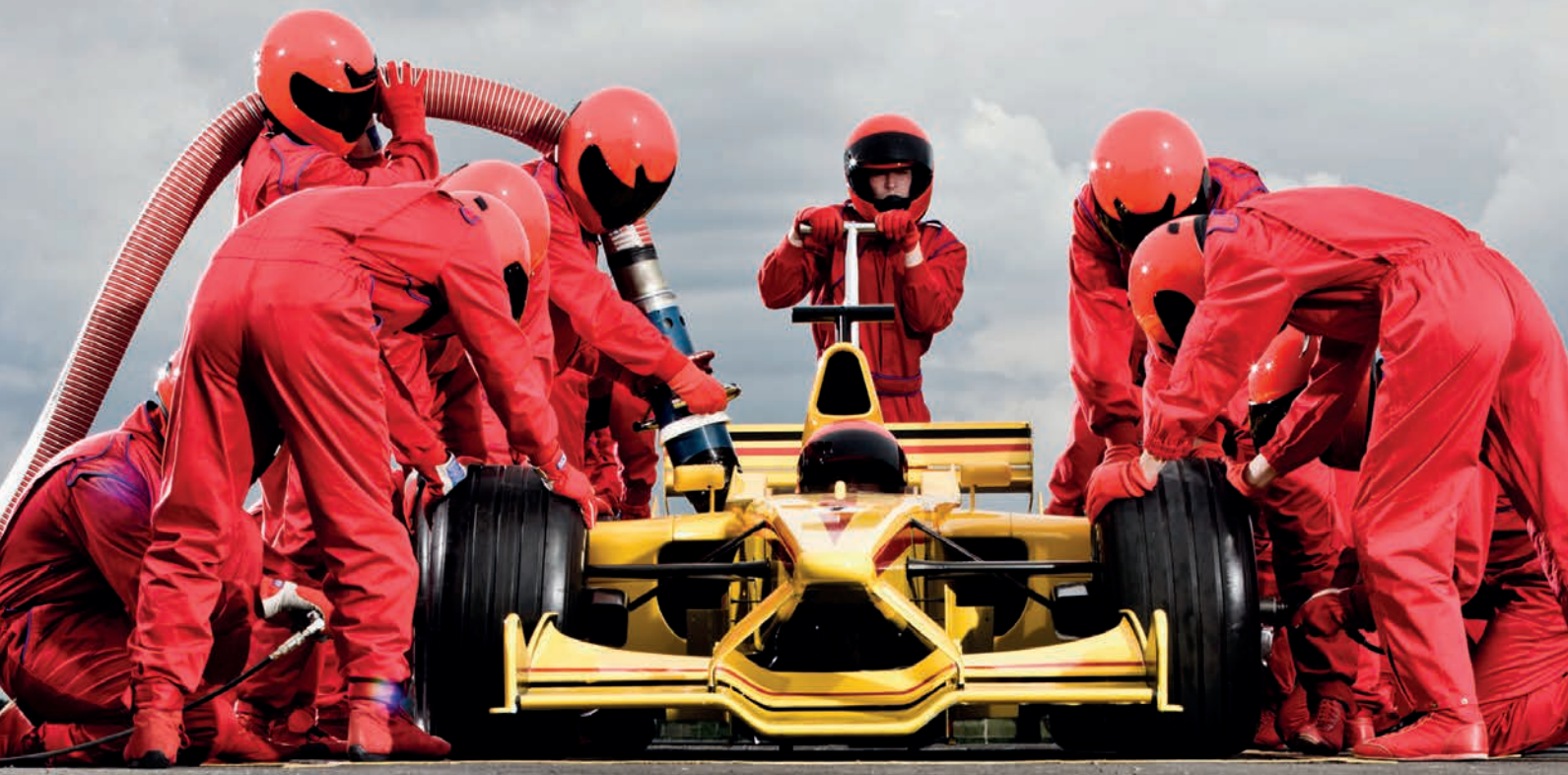
Public management letter



Managing risks is a people's business

Risk management and reporting in large enterprises

November 2013

NBA

Nederlandse
Beroepsorganisatie
van Accountants

NBA

The NBA's membership comprises a broad, varied occupational group of over 20,000 professionals working in public accountancy practice, at government agencies, as internal auditors or in organisational management. Integrity, objectivity, professional competence and due care, confidentiality and professional behaviour are fundamental principles for every accountant. The NBA assists accountants in fulfilling their crucial role in society, both today and in the future.

To stakeholders and interested parties in the theme of
Risk management

P.O. Box 7984
1008 AD Amsterdam
Antonio Vivaldistraat 2-8
1083 HP Amsterdam
T +31 20 301 03 01
nba@nba.nl
www.nba.nl

Date
27 november 2013

Re
PML Risk management

Direct dial number
020-3010302

Dear Sir, Madam,

Risk management is a relatively new discipline which in recent years has become of public interest. Larger enterprises even have a separate department and include a risk management paragraph in their annual report. And yet companies still get into difficulties. So is risk management the correct approach in order to stay out of the danger zone? Would there have been more corporate scandals if less attention had been paid to the subject? What is risk management in fact? All questions which accountants have to deal with. Good risk management also prevents errors in the annual accounts, focus of the accountant's audit.

Nederlandse
Beroepsorganisatie
van Accountants

NBA

In this public management letter (PML), the Netherlands Institute of Chartered Accountants wishes to contribute to the development and discussion of risk management. The five signals and recommendations are intended for directors, Supervisory Boards, stakeholders, accountants and other interested parties in large companies. But the public and SME sector may also benefit from it.

Our signals:
1. Managing risks is a people's business
2. Risk appetite is not well-defined
3. Embedding in the enterprise is insufficient
4. Risk paragraph is incomplete
5. Accountants pay little attention to risk management

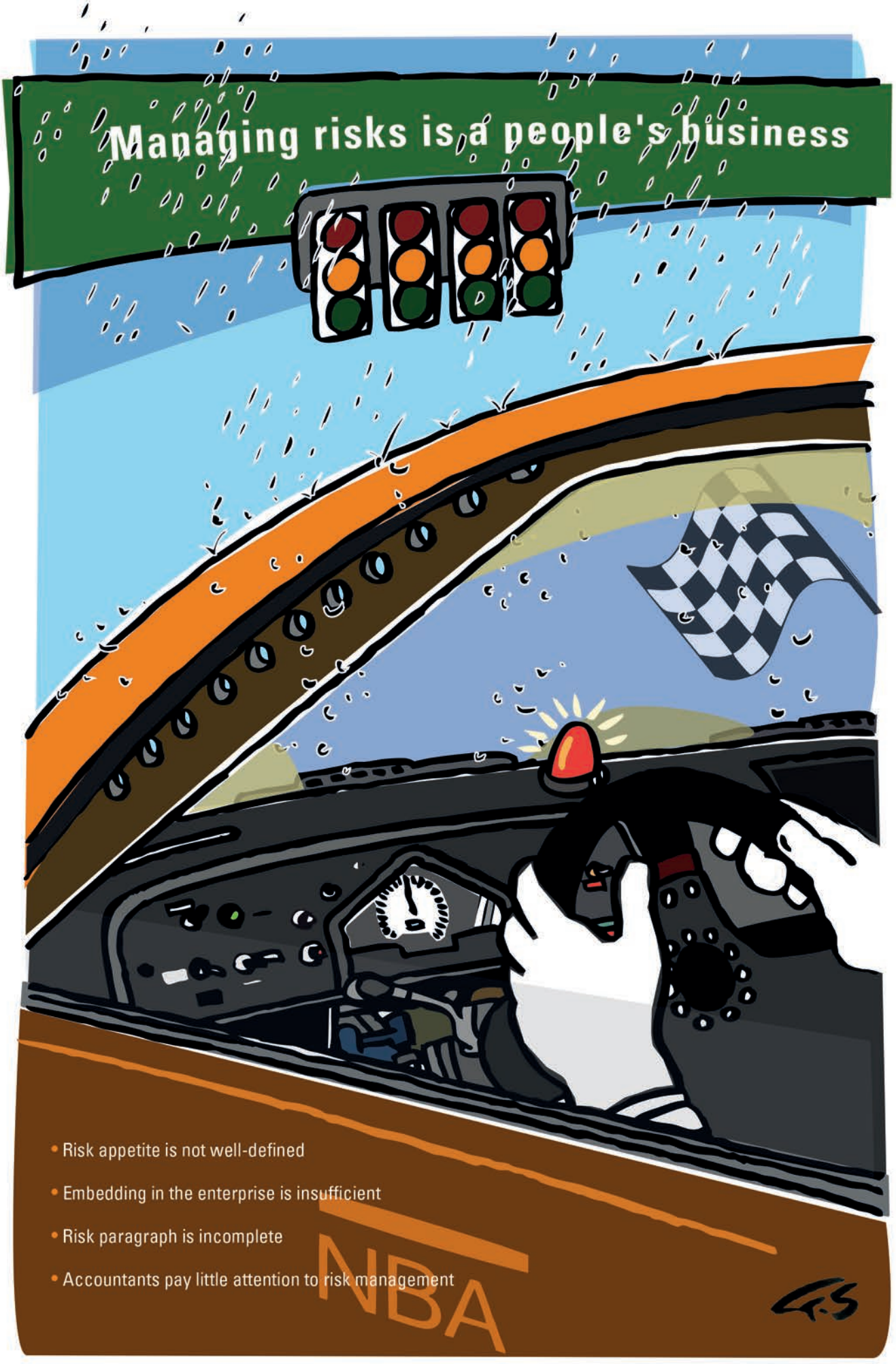
Risk management is more 'art' than 'science'. How far should that go? Should the risk manager have right of veto in important commercial decisions? In doing so he himself becomes a director. But even if that right of veto does not exist, risk management very quickly becomes an interference. The main problem lies in the elusive element inherent in risk management. Probabilities, risks, results, checks, in various countries and sectors. It is useful to address the great uncertainties of risk management. Everyone struggles with the concepts: directors, audit committees and accountants. Everything is outlined formally and neatly. But it works out different in practice. Risk management is intended to manage uncertainty better. Proper understanding only results from comprehensive dialogue, with respect for this practice.

This PML is based on the expertise of our members who are involved with the theme. Various stakeholders, including NNR, Eumedion, VEUO and IIA Nederland have provided us with their comments. We are grateful to all of them for their contributions.

Yours faithfully,

drs. Huub Wieleman RA
chairman NBA

Robert Jan van de Kraats RA
member NBA Identification Board


Managing risks is a people's business
• Risk appetite is not well-defined
• Embedding in the enterprise is insufficient
• Risk paragraph is incomplete
• Accountants pay little attention to risk management
NBA

Contents

Risk management: just a formality?

What is risk management?

Risk management has never received so much attention as in the last twenty years. Following a number of catastrophes in publicly listed companies the call is growing for risk management to be taken more seriously. But what do we understand by that? According to COSO[1] it is an ongoing management process[2] within the company.

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

In this description, risk management has a negative undertone. Business is all about taking risks, but also profiting from opportunities. Risk management is also important to that other side of the coin. Ultimately it's about the right balance between risks and return.

Due in particular to the Dutch Corporate Governance Code[3] risk management has come high on the agenda of executive and non-executive directors. The code requires directors to periodically evaluate the risk management system and discuss the results with the Supervisory Board. Management must also declare annually that it is 'in control' via an In Control Statement. This works out different in practice hoewever. In a recent study of Dutch companies[4] one of the conclusions is that risk management is still in its infancy.

Reports are meaningless

According to non-executive directors and chairmen of the board, risk management belongs in the top three items for the Supervisory Board[5]. It can be assumed that this is also the case for investors and that companies take their needs into account. However, reports on risk management in annual reports are often perceived as meaningless by institutions such as Eumedion and VEB. This is noteworthy, as the annual report is required by law to contain a description of the principal risks and uncertainties with which the company is confronted. In practice, many questions remain unanswered, such as: what risks does the company wish to accept, what happens in practice, what are the consequences if it goes wrong and how does the organisation deal with threats? The reports contain a great deal of text but say very little. Risk paragraphs of more than ten pages do not achieve their goal.

Even directors of companies question the need for and usefulness of risk management, despite the investments in it during recent years. These investments were mainly to do with the management of operational risks. Risks in operational processes, financial reports and compliance with legislation. In short, known sources of errors. For directors, other risks including reputation risk are more interesting. Questions in the field of strategy, competition, technology and changes in market demand. These are still known risks, but at a higher management level. Even more difficult are the questions surrounding unknown, uncertain events in the future. For example a credit crisis, technological innovations and climate change. Unknown risks at a high level of abstraction, usually in the long term. Risk management systems are still too focused on operational problems,

1 Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal control- Integrated Framework (1992).
2 Management must be broadly interpreted: COSO distinguishes 4 types of response to a risk: reduction (control), acceptance (take), avoid (terminate) and transfer (transfer).
3 The Dutch corporate governance code (2003, amended in 2008).
4 Nyenrode, RUG, PwC and NIVRA: risk management in times of crisis (November 2009).
5 Prof. dr. F. van Eenennaam, Dynamics of Strategy, The games of Competitiveness and Corporate Governance (2006).

whereas directors have need for strategic risk information. In management meetings with the Supervisory Board, risk management is a standard agenda item. From the point of their supervisory role, non-executive directors need to know if the company is still in control.

The human factor overlooked

It is evident from many studies that in the event of uncertainty, decision-making does not take place (fully) in accordance with assumed rational principles. In the assessment of investments, people are often risk-averse. They hesitate to accept their loss or to acknowledge that something has gone wrong. It then becomes difficult to see the true picture. The investment amount gets an uneven weighting in the consideration of whether a project should be stopped or allowed to continue. In those circumstances, people often overestimate the possibility of managing risk. The human factor in risk management is easily overlooked.

Current risk management does not speak the language of directors very well. Risk managers are all too often involved in operational issues and use jargon which is distant from actual business. People who fulfil the risk management functions rarely sit at the table when strategy is being determined. They tend not to possess the knowledge, skills and authority to act at that level. Risk managers often apply operational techniques which are less suitable to strategic risks. For example in decisions to expand into particular countries, in complex financial strategies, large acquisitions or new markets. Risk management therefor does not lead to more effective decision-making by management.

There may also be a silo approach within the Board of Directors. Significant risks usually exceed the field and competencies of individual businesses or functions. Proper cooperation between them is therefore essential. According to some experts, risk managers should pay more attention to the development of new techniques, such as scenario-analyses, stress-testing and calculating effects of more or less risk appetite. Risk management is a new discipline into which little scientific research has been done. There are no generally accepted norms. This makes it difficult to provide value assessments on the quality of risk management.

Does the accountant leave out chances?

And what is the role of the accountant? Is he, in football terms, the cover-all controlling midfielder? In society, accountants have been assigned the role of gatekeeper: identify relevant threats timely. But whether this means that he provides assurance on the quality of risk management is still a subject for discussion.

In any event, the accountant plays a significant role in the risk management system. In particular in the annual accounts audit, assessment of the risk paragraph in the annual report and via the management letter. But in view of the interests of risk management to directors, the question is whether he does not leave out chances in this area.

Signal 1 | Managing risks is a people's business

Soft controls are the intangible side of risk management, the human factor. Measures which have an effect on culture, conduct and motivation of employees. Conduct determines to a large extent the success of risk management: what stimulates an employee to take certain risks or not? In practice the emphasis lies too much on hard management measures.

In further detail

When implementing risk management companies are often quick to place the emphasis on tangible measures. For example on an extensive description of all risks, the appointment of a risk manager and the establishment of practical management measures. Risk management however is not just about risks at a management level. Consideration of whether to accept or avoid a risk takes place every day by employees in the work place, during their everyday activities. Employees must possess the right knowledge, experience and tools to make conscious choices in the interests of the company.

Hard, specific measures are demonstrable and measurable. They only work however if employees are motivated and incentivised to apply them in practice. This is the area of soft controls. The five most important elements are:

- **Leadership and role model behaviour.** This is also called tone at the top in a company. Employees must get the feeling that risk management is important. Management must provide a visible good example where risk awareness and risk management are concerned. This is true both within the company and outside of it.
- **Communication and information.** It must be clear to everyone what risks are desirable and what are undesirable, whether they match the strategy and risk appetite of the company and what the potential consequences are. Instructions in this area must be unambiguous and accessible.
- **Motivation and valuation.** This involves the creation of a pleasant working environment, in which employees can achieve both organisational and personal objectives in the area of risk management. Employees must be motivated and feel valued in the choices they make.
- **Stimulation and facilitation.** This focuses on promotion of cooperation, exchange of information and accepting individual responsibility. Reporting of errors in order to learn from them is encouraged. This ensures that the interest of risk management is shared and that employees feel called upon to make independent choices.
- **Approach and enforcement.** There must be clear thresholds between desirable and undesirable conduct. Employees ought to know what measures are taken in the event of undesirable actions. It must be possible to report abuse.

A risk management system which pays insufficient attention to the human factor is doomed to failure. Soft controls are necessary in order to allow hard management measures to work. That's why the accountant auditing the annual accounts must also pay attention to culture and conduct.

Negative example

No attention paid to workers' experiences

Company A has started to inventarise business and financial risks in order to create a risk framework. A opts to allow only management to take part in this project. In the analysis, management totally ignores risk-awareness of employees and the way in which they are guided in this respect. Insight into existing risks is unilateral and not focused on soft factors in the company. When A presents the framework, employees do not recognise the risks and the project is threatened with failure.

Positive example

Soft controls identified as a risk in restructuring

Company B wants to make a thorough risk assessment within the context of a restructuring. All employees are involved via special sessions. In these discussions the effect of culture and conduct on the effectiveness of hard measures and procedures was discussed. According to employees and management risks mainly concern the loss of motivation and loyalty and creation of unrest due to unclear communication. Therefore explicit attention was paid in the restructuring plan to approaching and addressing employees. Communication from management provided them with full clarity. The restructuring was a success.

RECOMMENDATION 1: Do not forget culture and conduct

- Acquire insight into the culture and conduct of employees, for example via an employee satisfaction survey. Risk management must be fine-tuned to the target group: the employees who decide on a daily basis to take or avoid a risk. Establish their levels of knowledge and experience and whether they have the right skills to make the correct assessment in the interest of the company.
- Provide a culture in which employees share their experiences and mistakes and discuss dilemmas. Involve HR and Internal communication departments in this. In a blame culture employees are more inclined to cover up mistakes. As a result the company cannot rectify mistakes and employees cannot learn from each others' mistakes.
- Apply the correct soft controls. Ensure that employees know what is expected of them and set them the right example. They feel motivated and know what the consequences of undesirable conduct are. Avoid a culture of fear.
- Pay periodic attention to risk awareness amongst employees. Ensure that they are aware of new developments and give them the opportunity to keep their knowledge and skills up to date. Provide training in subjects such as competition, export controls, safety and environment. Create a permanent contact point for their questions and concerns about risk management. Promote joint discussion of daily dilemmas.

Signal 2 | Risk appetite is not well-defined

Risk appetite forms the basis of risk management. Clear communication about risks a company is prepared to take is of great importance. Practice indicates otherwise. Risk appetite is not well-defined or not in line with corporate strategy. This has a negative effect on management and therefore on being in control of the company.

In further detail

By definition, business involves taking risks. Swift and appropriate response to changed market conditions, new opportunities and developments. An enterprise runs greatest risk at the moment that it does not move with the market. Taking risks without clear agreements about limits to be observed is hazardous. Risk appetite therefore provides guidance for corporate strategy. It states what level of risk a company is prepared to accept in order to achieve its objectives. It must be linked to strategic choices made and must have thresholds and limits, according to various risk categories[6].

In practice, the need to define risk appetite clearly is not always felt. Practical interpretation creates problems and can be divided into four types:

- **Non-explicit.** There is no clear picture of the company's risk appetite.
- **No match.** Risk appetite does not match with company characteristics and needs, interests and rules of various stakeholders.
- **Not unambiguous.** Risk appetite is not clearly and unambiguously defined and no consistent picture comes to the fore for the whole enterprise.
- **Not known.** The Board of Directors has established risk appetite, but not communicated it to company employees.

Expressing risk appetite in financial terms is certainly not straightforward, but it begins with a description of the thought processes followed, dilemmas involved and considerations made.

Lack of clarity on risk appetite has a detrimental effect on effective control and management of the company. If foundations of the risk management system are not sound enough, the entire system cannot function effectively. The company is then not in control, despite all measures taken. The company's employees and stakeholders do not know where they stand. If the level of risk the company is prepared to accept is unclear, it is difficult for them to take decisions. It is therefore appropriate for the auditor to pay attention to the company's risk appetite.

6 Strategic risks, Financial risks, Operational risks, Compliance risks and Reporting risks.

Negative example

Risk appetite remains vague

Company C is a trading company which has not clearly established how much risk it is prepared to accept in its various strategic aims. A certain form of risk appetite is apparent from various documents, reports, plans and even verbal statements, but this is extremely vague. It was stated in a strategy document that, in the years to come, acquisitions in certain global regions would be necessary to enable growth. Various risks to achieving this objective were outlined, including that of political stability. But nowhere did C state the precise risk appetite on this point, let alone that this was accessible centrally in the organisation. Neither employees nor stakeholders had a clear idea of C's risk appetite in terms of its strategic aims.

Positive example

Rik strategy clearly established

Company D is a production company which has not only established in its strategy what risks it is running but also how far it is prepared to go on each identified risk. This is laid down in the risk strategy. D states who determines risk strategy, what is taken into consideration in doing so and how often risk appetite is reassessed. In doing so D has named sustainability as a strategic aim. To this end D has assessed risks in terms of health, safety and environment (HSE) in order to be able to subsequently manage this. D does not wish to market any products which may harm consumer health. Risk strategy is made clear to relevant departments in the company, including via workshops. Together with management, these departments determine how risk policy can be linked to aims and risks at department level. Each department has included risk appetite in its own systems, procedures and working arrangements. Departments report periodically to D's management.

RECOMMENDATION 2: Make risk appetite clear

- Link risk appetite to long term strategy. Allow risk appetite to form part of strategic decision-making. Establish a link between strategic aims, risks and risk appetite. Communicate this clearly to employees and stakeholders in the company, by describing risk appetite on the company's website.
- Quantify where possible, qualify where not possible. The more specific the formulation of risk appetite, the more insight it provides. Quantify in bandwidths in order to prevent any under- or overestimation. Use a qualitative description if quantification is not possible. Make risk appetite specific to various risks or risk categories.
- Place risk appetite explicitly on the Board of Director's agenda. They determine the level of risk appetite. Allow the risk management department to play an advisory role. Ensure that risk appetite is regularly reassessed if circumstances within or outside of the company change. Link this to the periodic update of strategic aims.
- Ensure alignment between various elements of internal risk management. Risk appetite must not only be linked to company's characteristics and its environment, but must also be embedded internally. This means for example a translation to the company's core values, authorisation limits, procuration and mandates and linking the internal audit programme to the risk profile.

Signal 3 | Embedding in the enterprise is insufficient

Risk management is an essential tool for achieving company's objectives in a structured and managed way. As a result risk management has many interfaces with governance, planning and control. Nevertheless many companies set up their risk management as an individual and isolated process.

In further detail

Governance relates to organisation and control of a company, including the accompanying lines of reporting and accounting. A good planning and control cycle provides an important safeguard for reliable information on results achieved. Risk management also focuses on achieving company's objectives, but especially on management of associated risks. Its embedding in governance, planning and control at every level of the company is therefore to be expected. In the annual accounts audit, accountants need to pay attention to the way in which risk management is embedded in the company.

How this embedding takes place depends on many factors. For example, the scope and complexity of the company in its products and services, sector type, company culture, maturity or life cycle of the company and applicable law and regulations. Sectors which have long been strictly regulated due to consumer protection or high safety or environmental risks are at the forefront of attention paid to risk management.

Whether this embedding is successful is strongly influenced by quality and expertise of employees involved in risk management. A great deal of expertise about risks is present in the work place and with line management. If there is insufficient connection with this, the risk management function is destined for isolation. Due to lack of expertise and clear information, it is then not in a position to provide required control information at management level. As a result its role in the overall decision-making process is restricted.

The company's remuneration policy is rarely linked to risk management. The way in which directors are remunerated is a cornerstone of the company's governance structure. In order to establish a link between performance and risks taken, the monitoring of risks must take place in the planning and control cycle. That is only possible if risk management forms an integral part of that cycle. Performance indicators in remuneration policy are often financial in nature. As a result they can easily be compared with external data. Risk indicators are primarily qualitative in nature because they often cannot be expressed in financial terms. As a result of this, external comparison is less straightforward.

It occurs all too often that risk management is interpreted as a separate, isolated process, alongside primary operating processes. As a result, it is too distant from the daily course of events and is not a partner in dialogue for management. In fact the role is all played out before the game has begun.

Negative example

Risk information not shared in planning & control

International company E has an extensive country structure. Branches operate relatively autonomously. Financial information is compiled locally and forwarded to the head office in the Netherlands. Information is consolidated there on a monthly basis. Risk analysis is also carried out locally but results were not shared with the central risk management function at head office. As a result, head office does not have full insight into the risks for each branch and potential joint dependencies. This renders E vulnerable, because it is inadequately prepared to react quickly to local risks.

Positive example

Management applies integral approach

Company F is active in a risky sector. Physical safety of its employees is paramount. The company has traditionally focused on accidents prevention. This is accounted for, both internally and externally. This focus led to early realisation by F that risks can only be managed effectively via an integrated risk management programme. Although physical safety received the most attention initially, financial and other operational risks have subsequently been incorporated. F's information system is set up for this, risk management is an integral element in the planning and control cycle.

RECOMMENDATION 3: Do not view risk management as an isolated theme

- Ensure that risk management is integrated in the planning and control cycle. The determination and monitoring of risks is not only a task for risk management, but in fact for every manager. Carry out a joint evaluation with the Board of Directors at least once per year. Share these evaluation results with the Supervisory Board.
- Embed management of strategic risks at the top of the enterprise by assigning a significant role to the Supervisory Board.
- Enhance the knowledge of established risks within control and risk management functions. Ensure a better balance between line management and control functions. Arrange for the risk management function to have direct access to Executive and Supervisory Board.
- Embed the role of risk management in the decision-making process. Ensure that everyone who is part of that process has access to all risk information. This also applies to the Supervisory Board.
- Research the possibility of establishing a direct link between remuneration policy and results of the risk management process. Attempt to establish a link between performance and risks taken. Seek potential performance and risk indicators. Involve the Supervisory Board in this.

Signal 4 |
Risk paragraph is incomplete

The risk paragraph in an annual report is the means of communication of risk management to the outside world. Stakeholders have been indicating for years that they require more information about the company's strategy and the associated opportunities and threats. However, risk paragraphs are still too general, too concentrated on negative risks and inadequately future-focused.

In further detail

The basis for the risk paragraph is laid down in various reporting regulations. Both Book 9 of the Civil Code and Dutch Accounting Standards require inclusion of risk information in the annual report. The Dutch Corporate Governance Code also imposes requirements in this area.

The risk paragraph forms part of a company's annual report. The section usually consists of a description of risk profile, the way in which the company deals with risks and an In Control statement by management as the final document in the risk management process. Further analysis of risk paragraphs[7] of large, publicly-quoted companies indicates that essential requirements are still lacking:

- Cohesion between strategy, risk appetite and management control system is lacking.
- The risk paragraph concentrates too much on the past and not enough on the future.
- Risks described are principally negative in nature. Moreover, they are too general, bear little relevance and are not adapted to company characteristics. Questions such as what is meant by a specific risk and why it is relevant are not answered.
- Effect of the risks described is inadequately explained. The risk paragraph does not address the effect for the company if it goes wrong.
- Risk appetite and management measures taken are not (clearly) explained. The question of what a company does to reduce a risk or why it does not wish to do so remains unanswered.
- Companies often use too many standard texts which are not specific enough.

Directors therefore miss out on the opportunity to connect with stakeholders, to show what business is truly about. Whereas stakeholders, in particular shareholders attach great importance to clear information about strategy, opportunities and threats. How much risk can a company allow itself, how great is the damage if it goes wrong and what does the company do about it.

Companies are extremely reticent to provide such information. They consider the information to be commercially sensitive and liable to have a negative influence on share price. Many directors fear potential personal consequences should it subsequently appear that the risk paragraph did not state risks correctly. This leads to a box-ticking culture: the risk paragraph is no more than a formal exercise to comply with rules.

7 This is apparent from several studies including: Study of the risk paragraph in the 2009 annual reports of Dutch listed companies (NIVRA, October 2010).

Negative example

Meaningless risk paragraph

In its risk paragraph Company G addresses negative consequences of the economic crisis. In its description G usually occupies the role of victim. G refers to causes outside the company, over which it has no control. It does not indicate what its own role in the overall situation has been. The reader of the risk paragraph receives no response to questions such as: to which specific activities do risks apply, what can the company itself do about it, how will problems develop and is the company in a position to survive this? As a result the information value of the risk paragraph is almost zero.

Positive example

Informative risk paragraph

Listed company H, specialising in storage of chemicals and other products, has incorporated an informative risk paragraph in its annual report. H provides insight into its strategic objectives and associated risk appetite for each risk category, via a clear table. H then addresses its most significant risks for which it provides clear information about the way in which these risks are managed. H also cites specific examples of where things went wrong and the lessons learned. The risk paragraph concludes with an In Control statement from management.

RECOMMENDATION 4: Provide the reader with the risk paragraph he needs

- Do not consider the risk paragraph as a compulsory accounting report, but as a means of communication to inform stakeholders. Explain how the company earns its money and why appropriate risks must be taken in order to be successful. Be clear about risk appetite and the extent to which risks can be influenced. Limit the risk paragraph to a maximum of five most significant risks to the company.
- Provide strong insight into the risk management system and risks themselves for each risk category. Shift the emphasis from retrospective (explaining) to forward looking (anticipating). Make use of what-if analyses: state what the actions are if a particular scenario becomes reality. Also pay attention to non-financial aspects.
- Assign the Supervisory Board a more active role in compiling the risk paragraph. As counterpart to the Board of Directors it can provide a good contribution to a balanced and informative risk paragraph.
- Consider consulting the most important company stakeholders about contents of the risk paragraph. Inventarise their needs and establish if they can be met without compromising commercial confidentiality.

Signal 5 | Accountants pay little attention to risk management

Society expects accountants to provide an opinion not only on the quality of the annual accounts but also on the annual report. This includes a description of the quality of risk management. Given that expectation and in view of his signalling role, accountants would be well advised to pay more attention to risk management.

In further detail

Accountants' core task is to audit financial information, in particular in annual accounts. According to professional regulations[8] he must have an understanding of the company. In doing so he focuses mainly on reporting risks. He reports to stakeholders in the company and to society at large via the audit report. Within the company he communicates with the Board of Directors and the Supervisory Board. In publicly listed companies the accountant attends the general meeting of shareholders at least once a year.

In the audit, accountants pay attention to the quality of internal control related to the annual accounts and management's In Control statement, without giving an opinion on it. Risk management is also part of internal control, but the emphasis is on financial reporting. It is good to look at internal control in a broader sense, especially with regard to the quality of risk management and non-financial risk information. Non-financial risks also have consequences for annual accounts. It requires additional expertise in the audit team and additional audit budget, but it is possible. In practice however it is more difficult. Audit budgets are lean. Directors are often not keen on another view from accountants on the quality of risk management. The current audit report provides insufficient space. A better model is being worked on internationally[9]. Accountants however have to deal with liability risks and confidentiality. He will also have to invest in expertise. These are all issues which stand in the way of open communication with the outside world. Yet it is appropriate for the accountant to pay attention to this due to his public role. It is expected of him to signal if something is going wrong. Not paying attention to risk management is no longer of the moment. He can do enough without providing a direct opinion in his report. He can do this by asking a few simple questions:

- Does the company have a risk management system? How is that embedded? What is the role of the Board of Directors, Supervisory Board and internal audit function?
- Is attention paid to risk management in setting the company's strategic objectives? Does the company form a link between business operations and risk strategies?
- What risks have been identified by the internal audit function and what is its opinion of the quality of risk management?
- Does communication between management, Board of Directors and Supervisory Board function well?

Many accountants wrestle with the subject. They do not succeed in fulfilling the expectations of society and their clients. In October 2011[10] the NBA proposed that accountants' role and reporting should be expanded. A company identifies its risks, the accountant examines the management of these risks including reporting on it in the annual report.

8 Control standard (COS) 315: Identifying and assessing the risks of material misstatement through understanding the entity and its environment.

9 See the proposals of 25 July 2013 by the IAASB (International Auditing and Assurance Standards Board) for the new statement. The accountant covers the most important audit findings in his statement. From 2013 in England the audit report contains information on the most significant areas of risk in the audit. Several pilot studies have been conducted in the Netherlands over 2013.

10 NBA Advisory report 'Robust gatekeeper's role: More certainty in more informative reporting'.

Negative example

Accountant does not press ahead

X is accountant of company I. In the auditor's report X reports only on the status of risk management. He is not critical of the limited interpretation of it by I. Instead of signalling faults or making suggestions for improvement, he writes: "The risk management and internal control department places its focus on risk management related to internal control environment and the In Control statement. I works on taking risk management to a higher level and a more integral approach. We support this development".

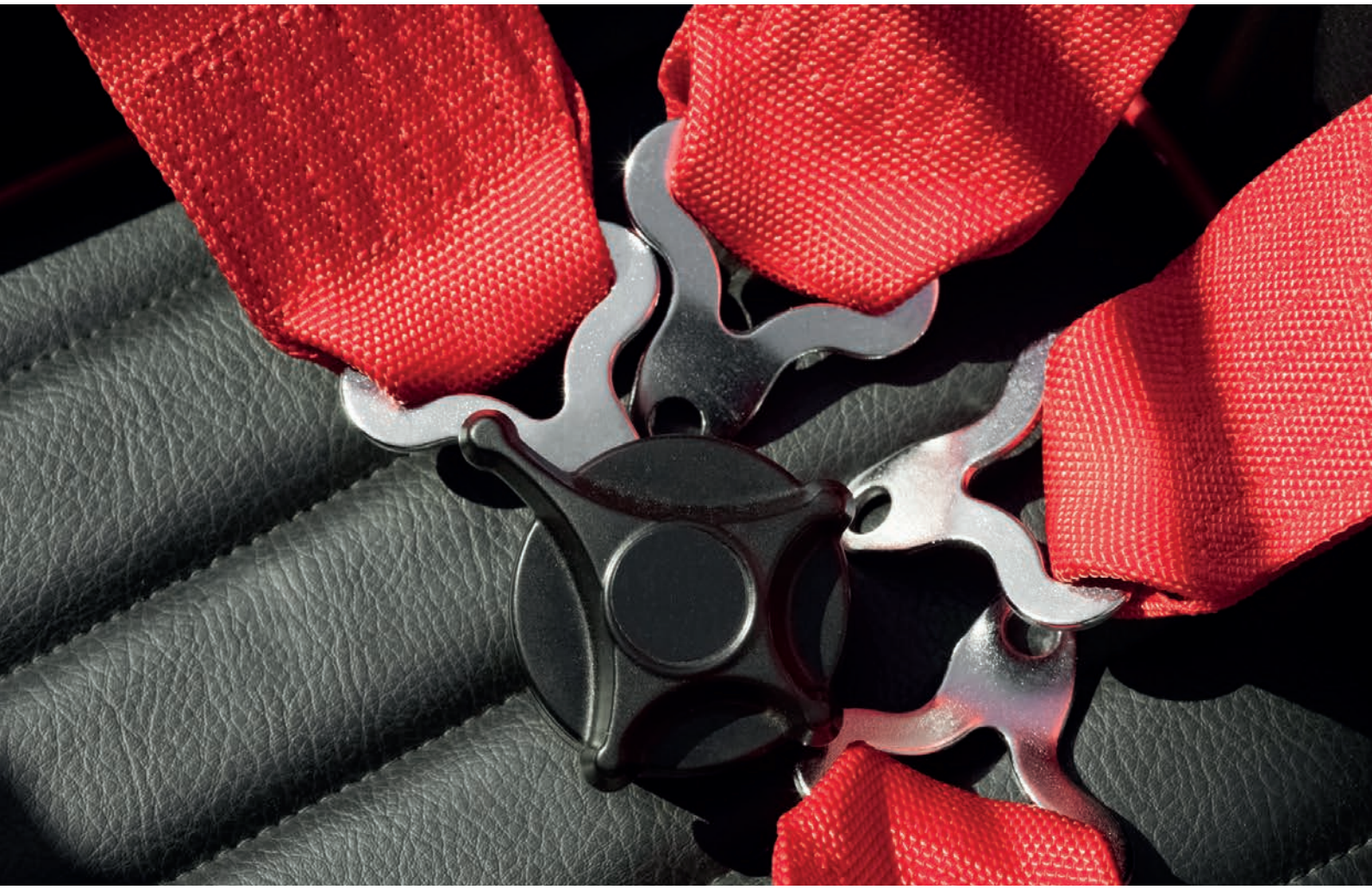
Positive example

Accountant is specific and provides his view

Y is accountant for construction company J. In the auditor's report Y is critical of J's risk management and of specific risks for a true and fair view in the annual accounts. Y reports the following: "Currently risk management focuses mainly on increasing risk awareness. We have found that an integrated risk policy, in which all significant businesses are involved, requires further development. The current assessment of risks is not related to company's strategic objectives. We also note that your annual reporting of risk management does not describe risk appetite in detail. With risk appetite clarity is given on the amount of risk the company is willing to accept. This improves effectiveness and efficiency of risk management".

RECOMMENDATION 5: Accountants, speak up

- Invest in expertise. Include a risk management specialist in the audit team. In the audit pay particular attention to the way in which a client identifies, manages and processes risk in the risk paragraph. Also evaluate the means of communication.
- Regularly discuss risk management quality with Board of Directors and Supervisory Board. Do not only discuss risks in the area of financial reporting. Persuade them to provide more openness on risk appetite and risk management in the annual report. Advise them to discuss the matter with major stakeholders.
- Consider providing more information on risk management quality in the audit report. For example in a section 'other matters' or by expanding the passage on compatibility of annual report with annual accounts.
- Audit firms support your accountants in the area of risk management. Set up an expertise centre, which they can approach with their questions. Develop a communications strategy: how far do we take commenting on risk management quality in the audit report? How do we communicate internally? Only verbally or also in writing? What is important to our clients and how can we support them in this? What does society expect of us?



Summary of stakeholders' responses

At the request of the NBA, four stakeholders in the field of risk management have responded to the public management letter. Their responses have been incorporated in their entirety in the Dutch PML. What follows is a brief summary:

Eumedion (Corporate Governance Forum)

Eumedion appreciates NBA's choice for risk management as the subject of its PML this year. The risks which publicly listed companies are confronted with and the management of those risks have long been important themes for investors. Just as investors need to understand a company's results, they also wish to understand risks involved. Realistic and transparent reporting of risks contributes to maintaining trust of investors in a company and thereby the continuation of the company's activities. Eumedion has been saying for some time now that the risk paragraph of publicly listed companies should become more meaningful. Eumedion has noted to its satisfaction that the PML adequately covers the improvement points put forward by Eumedion and provides 'best practice' examples.

VEUO (Dutch Association of Listed Companies)

VEUO emphasises the importance of the subject of risk management and also welcomes the attention paid to it by the NBA. The signals described in the PML are endorsed by VEUO. However, the impression given in the PML that risk paragraphs are meaningless is not recognised. Within publicly listed companies a great deal of attention is paid to these reports. The quantification of risks recommended in the PML may lead to the risk of 'apparent accuracy'.

IIA (Dutch Institute of Internal Auditors)

In general IIA recognises the five signals and recommendations in the PML and inserts several footnotes. From the point of view of their supervisory function, supervisory boards and audit committees must arrive at an independent view on risk management quality. The PML does not adequately acknowledge this role and attaches too much significance to the assessment by the accountant. IIA also refers to the importance of the '3-lines of defence' model for the embedding of risk management within the company.

NNR (National Network Risk Management)

NNR has read NBA's PML with interest and regards the PML as a worthwhile contribution to the discussion on risk management and the accountant's role in it. Signals are recognisable and recommendations - and certainly the concepts and principles behind it - are endorsed. NNR inserts several footnotes to the five signals in the PML. Risk management is indeed a new discipline but has a very old history when it comes to applications. The role of the accountant may be overestimated in the PML. Accountancy training still pays too little attention to risk management.

Credits

Knowledge sharing in risk management
In the NBA Knowledge Sharing policy programme the expertise of accountants is collectively applied to signal risks early in social sectors or relevant themes. In doing so the emphasis is on management risks to do with the control of financial and administrative affairs. In this public management letter (PML) the NBA is presenting five signals and recommendations on risk management. This subject is the eleventh theme selected by the Identification Board of the NBA. A working group of public accountants involved in the theme gathered anonymised findings and discussed them. This was then discussed at a meeting with stakeholders. The Identification Board applied a social assessment to the signals. Stakeholders in the theme were willing to respond in writing to the PML. Coordination and final editing was provided by the Knowledge Sharing programme team.

More information
A public management letter is one of the publications from the Knowledge Sharing programme. The NBA previously published public management letters about Insurance (June 2010), Long-term Care (November 2010), Commercial Property (June 2011), Greenhouse Horticulture (November 2011), Municipalities (June 2012), Charities (December 2012), VET colleges (April 2013) and Transport & Logistics (June 2013). An open letter on Pensions (February 2011) and a discussion report about Tone at the Top (September 2012) have also been published. All publications are public and intended for a broad audience.

Sdentification Board
Prof. dr. mr. F. van der Wel RA (chairman)
H. Geerlofs AA
Prof. dr. M.N. Hoogendoorn RA
R.J. van de Kraats RA
L.A.M. van den Nieuwenhuijzen RA
Mw. drs. M. A. Scheltema

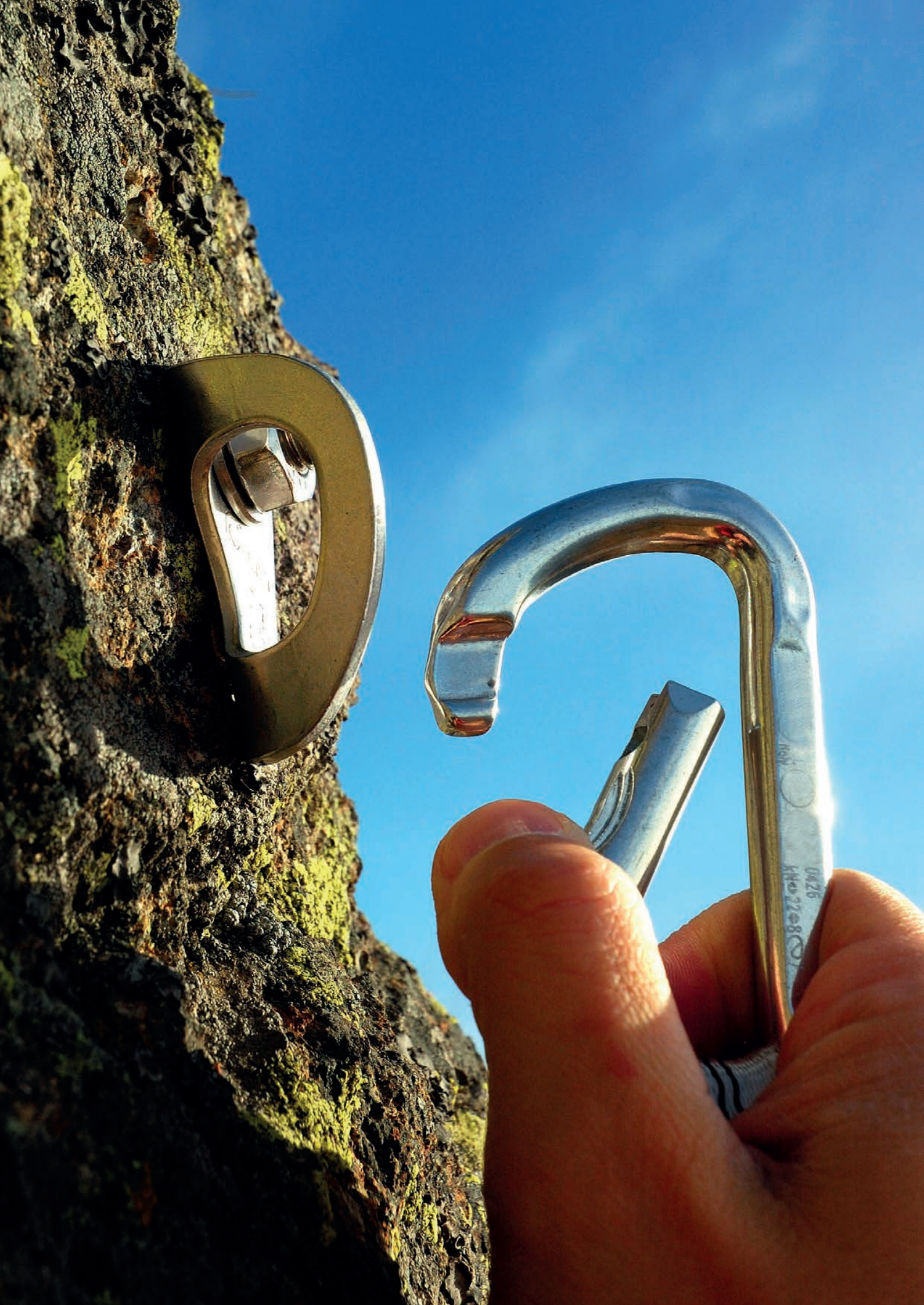
Risk management working group
W.T. Eysink RA CIA (Deloitte)
drs. J.H. Hijmans RA (BDO)
drs. L.H.A. Kreuze RA (KPMG)
Mw. drs. S.J.M. Mannaerts-de Swart RA (EY)
drs. J.K. Poot RA (BakerTillyBerk)
ir. M. Prinsenberg CIA (PwC)

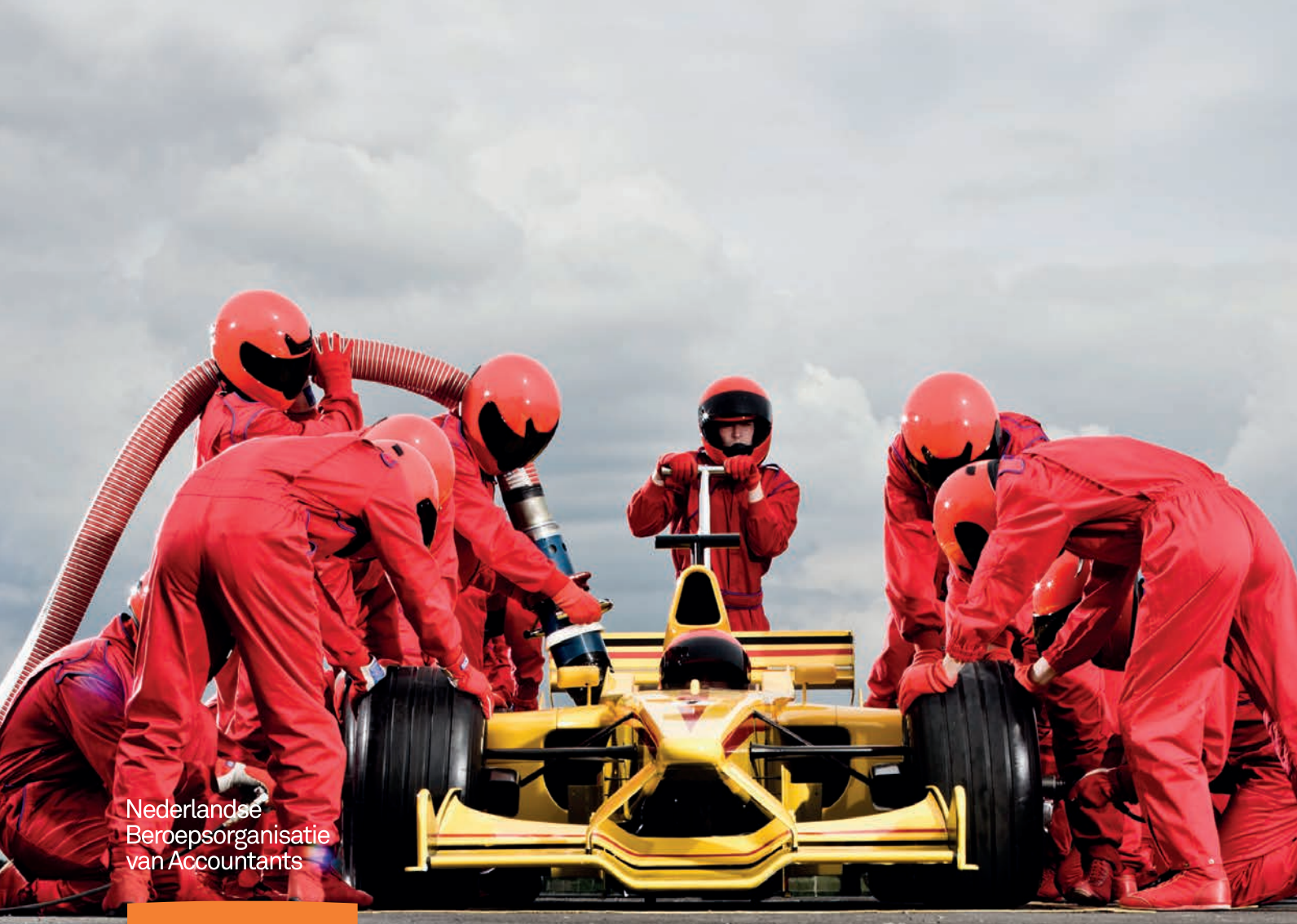
Knowledge Sharing Programme Team
drs. R.B.M. Mul MPA (chairman)
M.J.P Admiraal RA (editor)
J. Scheffe RA RO CIA
Mw. drs. J. Dankbaar

With thanks to
drs. C.A. Visser CIA CRMA (EY)
Prof. dr. L. Paape RA RO CIA (dean Nijenrode Business University)
drs. H. van der Wijk RA CIA (KLM)

Illustrator
Frank Strieder

Photo's
Dreamstime, Hollandse Hoogte





Nederlandse
Beroepsorganisatie
van Accountants

NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
F 020 301 03 02
E nba@nba.nl
I www.nba.nl