NETWORKED RISK MANAGEMENT

How to successfully manage risks
in hyperconnected value networks

TNO innovation for life

Rieks Joosten
André Smulders

NETWORKED RISK MANAGEMENT
How to successfully manage risks in hyperconnected value networks

TNO.NL

Authors
Rieks Joosten, rieks.joosten@tno.nl
André Smulders, andre.smulders@tno.nl

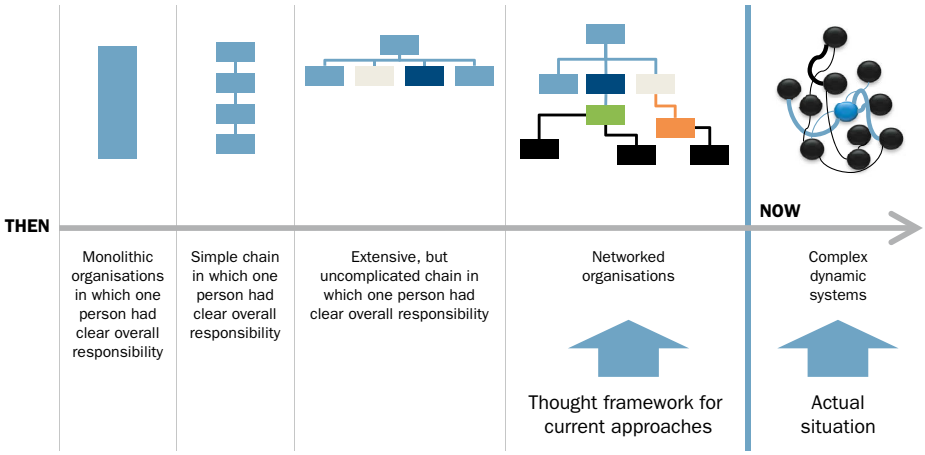
Editor
Taalcentrum-VU

Lay-out Coek Design, Zaandam

CONTENTS

1 INTRODUCTION

How do you manage risks as organisations and systems become increasingly complex and dynamic? This is a question that more and more organisations are trying to answer. Thinking in terms of risk is nothing new – it is part of our make-up. Nonetheless, it is clear that an ever-greater number of today's managers are losing control when it comes to risk management. It seems as though more and more work is needed in order to manage risks and to reduce the number of incidents. We have reached a point at which we need a new way to approach risk management. The existing concepts for managing risks are no longer suitable for the complex systems of which organisations now form a part.



The above diagram broadly shows how organisations have developed into complex systems. Organisations have evolved from clear monolithic systems into complex, networked, and adaptive systems.

From the perspective of how these systems are managed, they have already migrated to the latest model. This is because the organisations of which they form part are more and more often part of complex networks at different levels. This applies to operations and technology, among other areas. With regard to operations, it has long been commonplace for certain

aspects to be outsourced. The same thing applies to technology. The effect is that dependency on other parties, and disruptions experienced by other parties, have an effect on the particular organisation.

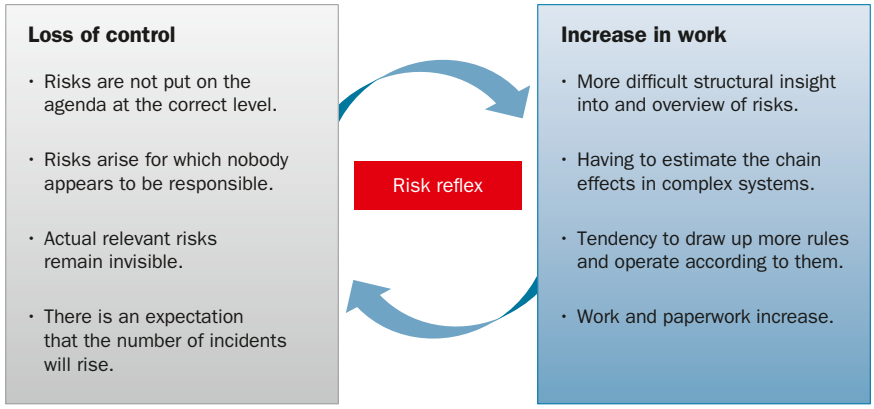
The world becomes more complicated as technology moves ahead. Organisations (and individuals) are outsourcing more and more, as a result of which they increasingly frequently enter into relationships with different parties using all kinds of communication channels. Each new relationship and each new opportunity – technological or otherwise – also entails new risks, while each change to a relationship or opportunity may entail a change to the risks concerned. It is also becoming increasingly important to be able to deal more quickly and more effectively with relevant risks in complex environments of this kind, in which various stakeholders have a part to play.

GUIDE FOR THE READER

The introduction describes the actual context within which a risk management approach has to be able to function. Chapter 2 describes a number of symptoms that provide an insight into the points on which risk management can fail. These symptoms, which we have repeatedly encountered in everyday practice, have prompted us to think about improving and developing existing risk management. In Chapter 3, we give a number of points where traditional methods are improved using Networked Risk Management. The basic terms and the starting point for success governance are described in Chapter 4. This is further elaborated in Chapter 5 into activities whose purpose and concrete results are specified. The Appendix has an alphabetical list of all the terminology that is used.

2 BACKGROUND: SYMPTOMS OF FAILING RISK MANAGEMENT

The way in which existing risk management methods deal with the complexity of today's work environment causes an unmanageable situation. This manifests itself through a number of symptoms, which can be divided into two main factors: the loss of control and the increase in the amount of work. The factors both exacerbate each other, with perhaps the risk reflex acting as a catalyst.
We define the risk reflex as the tendency to make new rules as a reflex response to an incident. This is shown in the diagram below:



2.1 LOSS OF CONTROL

One of the most important symptoms of loss of control is that the relevant risks are not placed on the agenda at the appropriate level. An example of this is a question to the ICT department of what risk a virus outbreak poses for the company's operations. However, the question should be expressed differently – what risks will arise if provision of the ICT

services is disrupted? Whether the disruption is caused by a possible virus outbreak or something else should not be relevant to the company's operations. It is then the task of the person or persons responsible for the company's operations to assess what risk operations is facing. They themselves have to ensure that they get an answer from the ICT department, and that answer then forms the basis for assessing the risk.

If an organisation makes no explicit mention of who is responsible for managing risks, risks will occur for which nobody appears to be responsible. This includes the risk of information leaks, for example – whose problem is this? And who should solve it? In many cases, the identity of those responsible for specific risks of this kind is given in implicit terms only, which means the risks remain unmanaged.

In addition, risks that are relevant to an organisation may stay invisible, because they continue to be covered at an inappropriate level. A one-off leak of information may be considered an acceptable risk for an ICT organisation, but what happens when the information could undermine the organisation's long-term competitive position? This is something that should be addressed at board level. In other words, if risks are not explicitly put on the agenda, or not raised at the appropriate level, the number of incidents is likely to increase.

2.2 INCREASE IN THE AMOUNT OF WORK

Most organisations make their risks transparent by analysing their complex systems and then listing the risks in that system. Although this approach involves the acknowledgement of the risks in complex systems, it does not mean controlling the risks in day-to-day practice. With the increasing complexity of the system and the related threats and vulnerabilities, it is inevitable that the amount of work caused by this approach will expand. The result is that it costs a great deal of effort to manage current risks. After all, you have to keep track of how the system is changing, be aware of new threats to all the parts in that system, and be aware of the options for tackling these threats.

This method is also reflected in the wish to make chain effects transparent. However, too little account is taken of the dynamics of a complex system, as a result of which rules are imposed that are based on temporary insights. These are intended to manage the situation that is presumed to exist at the time. On top of this, someone has to maintain and enforce these rules. This leads to more work and paperwork, which in many cases does not directly contribute to manageable risks. An example is that of security reports that make it impossible to determine whether there is a heightened or reduced degree of risk.

At present, the approach for managing ICT-related risks is rule-driven: the rules determine what is and is not allowed, and what controls should be set up. This approach may work for relatively simple and transparent systems that are closed off from the rest of the world (as was the case in the past), but is no longer useful in managing risks in complex and

dynamically changing environments. The more the proper functioning of such systems depends on different parties (stakeholders, whether in the same organisation or not) and changes to the environment, the more – apparently simple – things can go wrong, even if an entire security management framework is present in the organisation.

2.3 MIND SHIFT

At the same, an ever-stronger 'outsourcing' trend is emerging in the world around us. By this we mean giving genuine responsibility to employees, even though their freedom to act is limited to what is acceptable. In this form of 'outsourcing', services (electronic or otherwise) function on an increasingly stand-alone basis for multiple customers. You could also say that our society is organised more and more around networks, and no longer in linear chains. Whereas organisations used to manage their own fleet of vehicles, now they outsource this to organisations that also provide this service to others. People who in the past would spend their entire working lives in the employ of one single organisation nowadays work for different organisations every few years, or even for multiple organisations at the same time.

We would like to bring about a mind shift on the wave of this trend – that is, if a company outsources activities to one or more people, it does not matter if they form part of the company organisation or fall under another legal entity. In both cases, you are recognising that you do not yourself possess the expertise or competencies of the other party, but that you would like to use them in order to reach your own goals. For that reason, you make agreements with them and convince yourself that the risks that that entails are nonetheless acceptable to you.

The necessity for this mind shift is also expressed, albeit in different terms, in the Best Value Model of the Performance Based Studies Research Group[1] (PBSRG). The PBSRG claims that the mind shift means that less time and fewer resources are needed for managing customers and suppliers. It also creates the motivation to continuously improve, and enhances the sense of responsibility through performance measurements. Examples are shown on the PBSRG website.

There are two sides to the mind shift. The first has already been discussed: if we depend on someone, or choose to do so, this is because we believe that that someone is sufficiently professional and competent to do or supply what we want from them. The other side of the coin is that we ourselves have to work on our professionalism and competencies, so that others want to have what we do or supply. This means that we have to abandon the idea that there is someone above us (a sort of manager) whose wishes (or orders, as it were) we readily fulfil.

1 http://pbsrg.com/

If we accept this assumption, our success depends on the quality of our professionalism and competencies, and having control of the risks associated with that.

2.4 TURNAROUND IN RISK MANAGEMENT THINKING

Our practical experience tells us that there are various pitfalls in the area of risk management into which both large and small organisations tumble. This causes them to lose sight of the things that genuinely affect their results and to devote valuable resources to irrelevant side issues.

The feeling of being flooded by threats, vulnerabilities, and risks is a familiar one in this field. These are risks that you are barely able, if at all, to explain to the people who have to take decisions relating to them (board members, senior management, customers, etc.). In the case of information security, this effect is often enhanced by the increased dependency on and complexity of ICT – in the process, the risk management methods and concepts that have been used for many years keep us in their grip. Because we 'traditionally' apply these methods, we are partly preoccupied with matters that are not relevant to risk management. As a result, we are unable, or barely able, to explain ICT-related risks to managers or customers. It is hard to explain, either in advance or retrospectively, how risk management contributes to company results or organisational objectives.

It is on the basis of these observations and experiences that Networked Risk Management[2] (NRM) has been born. The result is a simple concept that helps target existing methods, tooling, and standards more effectively. It also offers handles for refining these aspects, where necessary. Below are the starting points we have used:

- The mission and goals of the organisation and/or managers are key.
- Risk management has to be easily understood, manageable, and workable for managers and others who are implementing it.
- Risks are related to the mission and goals of the organisation and/or managers.
- Decisions on how risk management is structured should be relevant and in keeping with these goals.
- Organisations (or parts of them) form part of a networked environment that is subject to rapid and frequent changes.

2 The terms 'El Metodo' and 'Advanced Risk Management' have been used as working titles in the past (in publications).

In saying this, we do not mean that risk management is insufficient in every organisation. We have used NRM to examine a number of organisations, which has shown that some are not only 'doing the right things', but also that they are doing them well. The NRM method helps in this process by making explicit the choices made, thereby making them accessible to a much wider audience.

2.5 THE PARADOX OF RISK VERSUS SUCCESS

Risk management is, of course, focused on risks. If there are not many risks, there is no point in worrying about them too much. However, if there are risks coming at you from all sides, then this poses great – sometimes impossible – demands on those who have the task of managing them. There is a paradox here – on the one hand, dealing with risks is useful or necessary to be successful and to attain objectives, but on the other, it also diverts the focus away from your objectives (and success). NRM helps you break out of this paradox, by assigning to managers and specialists alike the particular aspects of success and risk management that they can deal with and the implementation of which they are best suited to.

Everyone wants to be successful. Nonetheless, everyone goes about achieving success in a different way, because everyone has their own ideas about what 'being successful' actually means. We describe someone as successful if they reach their goals, or satisfy their needs; in short, if their actions only produce the results that they wanted. The same thing applies to organisations: they are successful if they fulfil their mission (their raison d'être) by supplying products or services, for example.

In our vision, risk management should serve success governance. This means that it should be possible to relate every risk to objectives that someone in the organisation has, as that makes the risk in question relevant to that person. Someone's success and the management of his risks then become two sides of the same coin. This also explains why checklists, of the kind commonly used in the traditional rule-driven method, do not generally work. After all, a person's or organisation's success – and therefore the risks – depends on the objectives that have to be attained, and they of course differ from one person or organisation to another.

We often define 'being successful' (in relation to people or organisations) in terms of the degree in which they better themselves. This is an important, but by no means unambiguous, starting point. There are organisations and people who regard someone as being successful if they do what their manager (the boss) says. In this type of organisation, individual initiative and responsibility are not, or not always, appreciated. This can result in inefficient, 'bureaucratic' behaviour, as once depicted in the OHRA advertisement featuring a

purple crocodile.[3] However, this method also places unreasonable demands on management, who after all need a complete overview of the organisation in order to be able to tell the people on the work floor what they have to do. It has been scientifically demonstrated that maintaining an overview of large organisations (or parts of organisations) is physiologically impossible for people; at any one time, people are unable to juggle more than seven (give or take one or two either side) balls in the air. Anyone who thinks they can manage more than that will make mistakes.

3 http://www.youtube.com/watch?v=mJipJwDPJ-g

3 NRM AND CURRENT RISK MANAGEMENT

Present-day thinking on risk management is determined by, among other things, standards like ISO 2700x (information security)[4] and ISO 3100x (risk management)[5]. The analysis in the previous chapters has revealed a number of deficiencies. When talking about 'Networked Risk Management', we are talking about a concept and method in which these deficiencies are being tackled. NRM refines the current way of working – and adds to it – thereby raising present-day risk management to a higher level of maturity.

Major additions or differences are:
1. the definition and the use of the term 'scope' (and 'context');
2. the use of tests for limiting the amount of work and for raising quality;
3. the distinction in NRM between obligation risk and expectation risk;
4. the support of NRM for making clear agreements (contracts, SLAs);
5. a more flexible way of carrying out the actual risk-management process.

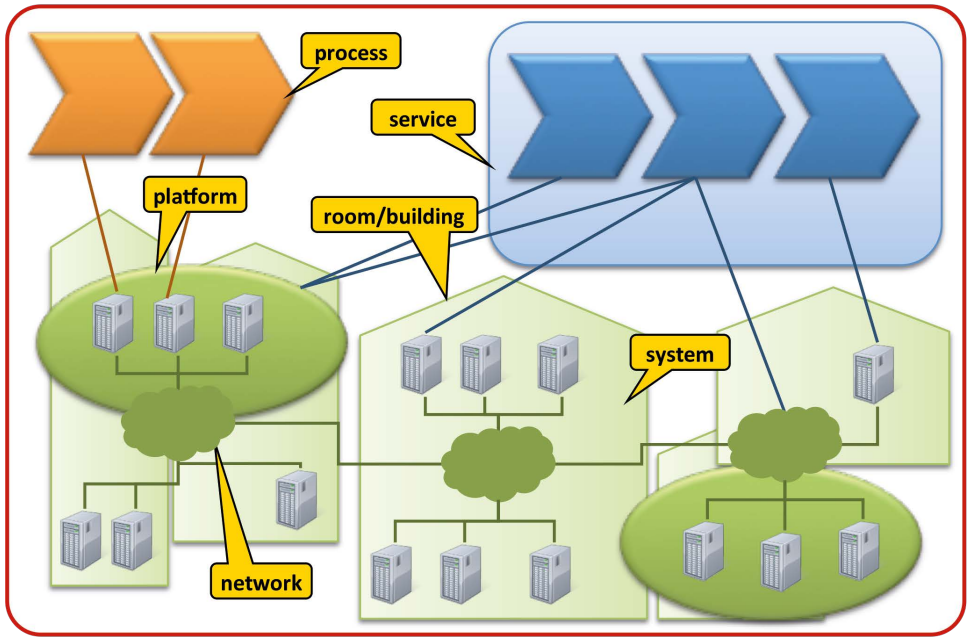
What these differences actually amount to and why they are important is set out below.

3.1 YOU DETERMINE RISKS IN A SMALL AND TRANSPARENT SCOPE

The term 'scope' is used to define an area that requires a specific type of attention. This definition helps people focus their attention on the things that matter (items that fall within the bounds of the scope). Other things (the 'context', see left) are then only considered to the degree that they are relevant to the things inside the scope.

4 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891
5 http://www.iso.org/iso/home/search.htm?qt=31000&sort=rel&type=simple&published=on

According to ISO 2700x and ISO 3100x, risk management starts by defining the area within which risks are to be examined.[6] For the assets[7] that fall within this scope, you determine the threats and vulnerabilities, and what risks they cause. The diagram below shows an example. The section marked in red is a scope in which everything needed for the purpose of providing a particular IT service is located. It includes processes, the support applications, the platforms and systems that they run on, the rooms or buildings where they are housed, and networks that provide the connections.



6 ISO 27000, Chapter 4.2.1.

7 The term 'asset' is defined as: 'Everything of value to an organisation' (ISO 27000, Chapter 2.3). It also states that there are many different types of company asset, such as information (see Chapter 2.18 of ISO 27000), software programs, physical assets (such as computers), services, people and their qualifications, skills, and experience, and 'intangibles' such as reputation and image.

The ISO standards assume that people know in practice how a scope or context should be determined, and set no requirements in relation to this. However, practical experience suggests that there is in fact a need for clearer definitions, not least because:

- it is often unclear where responsibilities lie and therefore who takes decisions regarding the risks relating to these responsibilities. The Scientific Council for Government Policy has acknowledged this in the civil service.[8]
- situations arise that encourage people to play troublesome games. A feature of service-oriented architecture, for example, is that different services use individual services, applications, and systems (and processes). If a system or process owner implements measures to cover the risks associated with one of the many services, then the other service owners will be pleased for the opportunity of a free ride. However, in many cases they will not wish to pay for it (after all, it is not something they need).
- scopes are often made so large that it is impossible to have an overview just of the number of assets inside them. Their interrelationships are then too complex to be manageable, and this is how human errors occur.[9]

NRM meets this need by defining a scope as the space in which one manager is responsible for fulfilling or complying with a number of interrelated obligations. If a large organisation with a board of directors is regarded as one scope, then every obligation will fall within that scope, and the board of directors will be responsible for complying with them and be held accountable for them. Examples include obligations towards the shareholders, the government, and others. A work process can also be regarded as a scope, providing there is clarity about the specifications that that process must meet (the obligations that must be complied with). There should also be a single manager with responsibility for meeting these obligations. If this is necessary, then it can be extended to the level of the individual: every employee in the organisation has obligations towards the organisation. They are set down in the contracts of employment, for example, function descriptions, and performance reports (targets that employees have to reach).

The idea is that the manager of each scope is able to oversee the obligations, and that this – for him – forms a manageable entity. This means that a board of directors can concern itself with the bigger picture, leaving the details to the managers of the various parts of the company. A process owner does not have to do everything himself: employees also perform tasks, allowing him to accept that his process will meet the relevant specifications. It could be argued that the individual employees have to do everything themselves, but they too are often assisted by secretaries, guards, HRM employees, planners, or IT systems, for example.

8 Scientific Council for Government Policy: 'Evenwichtskunst – over de verdeling van verantwoordelijkheid voor fysieke veiligheid', The Hague, November 2011, http://www.wrr.nl/fileadmin/nl/projecten/evenwichtskunst/2011-12-06__Evenwichtskunst__volledige_publicatie.pdf

9 James Reason, 'Human Error', New York, NY: Cambridge University Press, 1990.

3.2 TESTING FOR IMPROVING EFFICIENCY AND EFFECTIVENESS

After the scope has been established, in accordance with the traditional ISO 2700x/3100x risk-management process, an inventory has to be made of the assets. According to ISO, everything that is important to an organisation is an asset. However, for the purpose of attaining the company objectives, some assets are more important than others, and ISO also states that you should make an inventory of threats and vulnerabilities to the less important assets. Anyone who has ever carried out this activity will probably have felt that the task is pointless, at least to a degree. Having a means of testing the basis on which the importance of an asset for an organisation (and its objectives) can be established will help minimise the task of creating an inventory and therefore enhance the efficiency of the process.

After a list of the important assets has been made, an inventory must be drawn up of their potential threats and vulnerabilities. However, it is not necessarily clear whether something is a threat or risk, or a feature. Having a means of testing the basis of whether something really does form a threat or risk will contribute towards the efficiency and effectiveness of the risk management process.

NRM specifies different tests that are aimed at enabling the risk management process to run effectively and efficiently. The definition of the term ‘scope’ mentions the obligations (objectives) of a manager. You only have to make an inventory of your obligations to the extent that it is relevant to do so. The only reason for monitoring an obligation is if an unacceptable level of damage could occur were you not to fulfil it. Also, you only investigate the way your organisation fulfils an obligation if you need to do so in order to be able to make a sufficiently accurate risk assessment.

NRM specifies activities for specific goals that sometime are, and sometimes are not, relevant in the risk management process. You therefore only carry out an NRM activity if you need the result of it because you are aiming for such a goal. This makes carrying out the NRM process highly efficient and effective and is entirely in keeping with your needs.

3.3 DIVIDING RISKS INTO OBLIGATION RISK AND EXPECTATION RISK

Books, articles, and standards have different definitions of the concept of ‘risk’. One could concern an event that has an unintended or undesirable effect, such as a lightning strike. Another could relate to the occurrence of the unwanted consequence, such as a loss of power resulting from the lightning strike. The term is also used to designate the likelihood of such events occurring. This in itself gives rise to confusion. There are also documents that are not consistent in the application of their own definition: if we enter the relevant definition into every sentence where the word ‘risk’ appears, we will regularly encounter sentences or arguments that are incomprehensible. This only serves to make the confusion complete.

In NRM, the 'risk' has a clear meaning that is not only applied in a consistent fashion, but is also derived from what is relevant for managers. We see that wishing to (or having to) fulfil obligations[10] is the ultimate cause of every risk. This concerns not just obligations towards other people, but also those that a manager imposes upon himself.[11] The test of whether something is an obligation in relation to a particular scope is whether the manager of the scope in question recognises the obligation as such (in other words, that he accepts his responsibility for the obligation) and that he himself is adversely affected if the obligation is not met.[12]

Role of obligation risk

Not fulfilling, or not being able to fulfil, an obligation is a risk of the scope, or of the manager of the scope. How great that risk is depends on the degree to which the obligation cannot be met. This could also be seen as the product of the likelihood of this happening and the impact (the amount of 'pain' suffered) that it has on the manager.[13] These obligation risks are highly relevant to the manager, as they are directly linked to the obligations (goals) for which he is responsible. They also show which obligations should receive the most attention, and which first. This makes it necessary to make explicit the obligations associated with a scope (the obligations of the manager).

Role of expectation risk

To fulfil his obligations, a manager will not be the only one who actually has to work: generally speaking, will also be dependent on others. A board of directors can only realise the mission and other obligations of the organisation if there are parts of the company that do the operational work, the HRM, sorting out legal matters, and so on. A process owner can do some of his own work himself, but will depend on other managers for IT support or where adjacent processes are involved. This dependency on others is clear from the expectations that a manager has of other people. For example, the board of directors' expectations of the legal affairs department may be that the department maintains an up-to-date inventory of laws and regulations that are relevant to the company. The importance of an expectation for the scope (manager) is the degree to which the realisation of the expectation contributes to the fulfilment of the scope's obligations. For this reason, it is important to make explicit the expectations and their relative contribution to the fulfilment of the various obligations.

If a manager expects something of another scope, and that expectation is not realised, then this is traditionally regarded as a risk for the manager himself. This 'expectation risk' could be described as the product of the importance of the expectation for the manager and the

10 Such as business objectives and targets.
11 Such as the mission of an organisation, rules of ethics, principles of integrity, and moral requirements.
12 The consequence of this is that one party may not 'impose' an obligation on another party, if that party does not accept the obligation. For example, a law only becomes an obligation if the party that would have to observe the rule would be sufficiently penalised if he were to break it. The legislator can arrange this by setting a penalty.
13 This is not unlike the well-known formula: (Obligation)Risk = Likelihood * Impact. In NRM, this formula is applied to every obligation.

uncertainty of the other scope fulfilling the expectation. The importance of the expectations is the degree to which their fulfilment matters for the manager to be able to meet his own obligations. Expectation risks are highly relevant to the manager, because they tell him the factors on which modifications to the management of other scopes should be based and/or what other measures should be taken.

3.4 THE ROLE OF AGREEMENTS

We have noticed that contract or SLA templates sometimes leave space for agreements regarding quality, information security, and the like. In practice, the space is left empty or a standard text is added to it, in the final versions of the contracts. This suggests that people have difficulty in writing down what should actually be written down: what agreements should (and can) you make with others and how should they be reported on?

NRM suggests that an obligation that a manager has to someone else is only meaningful if that other person expects that obligation to be fulfilled. Conversely, something that you expect of someone else will only be fulfilled by them if they feel obliged to do so. In order to make this clear, you make agreements. An agreement between two parties can therefore be regarded as an obligation on the part of one towards the other, in accordance with the expectations of the other towards the first party.

It may be the case that you expect something of another person, but that they have no corresponding obligation. At that point, you are running a considerable expectation risk. To cover this risk, you could try making an agreement with the other person so that they feel obliged to realise the expectation. If this is not possible, then you have to get sufficient assurance that the expectation will be realised anyway, by placing the expectation with another party, or by looking for alternative expectations by which you can meet your obligations.

Conversely, do you have an obligation to someone else, but who has no corresponding expectations with regard to that? In that case, you can scrap the obligation without any worries – after all, there is no point in aiming to achieve goals that nobody is interested in.

For a scope manager, this makes it easy to manage his agreements with another party. He only has to check his expectations and obligations towards this other party and to find out the extent to which the latter has a similar obligation or expectation towards the former. It is a good idea here to pay some attention for each expectation on how certain you are (assurance) that the party is going to meet them. This is because it is relevant for the purpose of determining his obligation risks.

3.5 YOU DETERMINE WHAT YOU NEED AND DO – NOT THE WORKFLOW

The performance of work, including that of risk management, is generally modelled as a workflow. This means that all activities that are needed to do the work (in a predetermined sequence) are carried out. The idea behind this is that once the activities have been performed, the risks are under control, or managed. However, this is by no means always the case. Someone given the task of conducting a risk analysis (in a certain context) clearly does not know what the results will be and what conditions they should meet. Because the person assigning the task often does not know either, there is a risk of the work having no or insufficient effect.

Many people only manage their risks implicitly: they only take action if they have not slept well, or if they 'somehow' feel that something needs to be sorted out. Such action means that they manage their risks in a way that enables them to sleep peacefully again: the signals that action needs to be taken are once again on 'green'. People in this category do not use workflows – they respond to signals.

NRM is not dissimilar to this principle in that it specifies a number of processes and sub-processes or activities that have a clearly specified goal with tangible results criteria. Fulfilling, or not fulfilling, these criteria creates the signals that NRM provides.

Let us take the main NRM process, for example. The purpose of this process is 'to gain and maintain control of your risks'. The first part of this purpose (to gain control) has been achieved if you meet the following criteria[14]:

a) You know all your obligations of which it is possible that an unacceptable amount of 'blood could flow' (from which you may suffer stomach ache or sleepless nights).
b) You have made an assessment, for each of your obligations, of how great the risk is that you are not going to achieve them.
c) You have determined that these risks, taken together, are acceptable (bearable) for you.

Failure to meet any of these criteria is a signal that you do not (or not yet) have control of your risks, or that you have lost control of them. If your aim was to gain or maintain control of your risks, then each criterion that has not been met (this is a signal) informs you that not only is there work that still needs to be done, but also where it will lead to, namely, meeting the criterion in question.

NRM specifies different activities, each with a goal and one or more results criteria. The goal answers the question, 'to what end should I carry out this activity?', 'how is it useful to me?' The question is important because it shows the reason for carrying out the activity. If the

14 In order to achieve the second part of this purpose (to maintain control), you should check regularly that you still fulfil these criteria. If this is no longer the case, you should ensure that you regain control and thereby once again fulfil the criteria.

goal is of no or insufficient interest to you, then you simply don't carry it out. The results criteria answer the question, 'how do I and the person carrying out the activity know that the work is done?' The question is important because it makes clear to everyone what result will be achieved by the work in the activity.

You are also free you use your own work methods. To meet criterion B, one person may use gut instinct, while another may prefer to use an 'official' method. A third person may decide to use his gut instinct to estimate the risks associated with relatively unimportant obligations, and a more detailed method for high-impact risks.

To make easier the work that NRM users may wish to perform, a number of help processes have been specified. You can use them if you feel you need to know what the results will be. An example is the BIA process[15], which produces a list of obligations, with an estimate of the maximum damage for each obligation that is not met. This means you fulfil criterion A. The estimate of the maximum damage makes it easier to assess the risks, which is needed for criterion B. In the case of an obligation for which you cannot adequately estimate the risk, you can run the 'cover obligation' process. This will provide you with an overview of your expectations for fulfilling the obligation concerned. It could be that this is sufficient for you to be able to assess the obligation risk, as a result of which you will have resolved the obligation. However, it may also be the case that you wish to involve more details in assessing your risk. For this, too, NRM specifies processes that you can use.

As well as processes for being able to assess your risks, NRM also specifies processes that you can use to find out what agreements you should make with whom in order to maintain your risks at an acceptable level, and to estimate the degree to which these agreements will be honoured (assurance). You can immediately incorporate the results in Service Level Agreements (SLAs) and other contracts, or use them to draw up standards frameworks. You can also use them to specify the requirements that reports must meet, thereby enabling you to actually manage with the help of the reported information.

NRM continues to develop at a rapid pace. Research is already underway into the usability (are the intended goals actually used in practice?) and feasibility (are there any work methods, preferably already in existence, that produce the results required by the goal?) of a number of process descriptions. We believe that users of NRM also wish to achieve goals for which no process description is yet available. A possible example of such a goal is that of 'selecting the best option from different options by which an expectation can be realised'. This could occur in an innovation or change project. Wherever it is useful and desirable, NRM will be expanded with process specifications for achieving goals of this kind.

15 BIA stands for 'Business Impact Assessment'.

4 NRM STARTING POINTS

NRM helps you to ensure that the part of the organisation for which you are responsible will either become or remain successful, as the case may be. Below are the starting points you will be using. We refer to this as the basic information. Chapter 5 contains the actual method of approach in six activities.

4.1 KNOWLEDGE OF BASIC TERMS IS NECESSARY

Before being able to use the NRM method, you first need to understand a number of basic concepts. You will become familiar with these terms and concepts both below and during the course of this booklet. You will also discover what you can do with them. A full list of terms and concepts can be found in the Appendix.

TERM	DESCRIPTION
Manager	A person (or group of persons) with responsibilities. Examples: a process owner, systems administrator, director, board of directors, minister.
Obligation	A result for which one manager is responsible. He ensures that this result is achieved and/or maintained. Examples: 1. 'Security for society' is an obligation of the Minister of Security and Justice. 2. 'Everyday items affordable, special items accessible' is the mission of Albert Heijn, and therefore of its board of directors. 3. 'Like a good housekeeper, looking after the company resources that have been made available' is an obligation for every employee in every company that has formulate this policy. Note that policy rules that apply to different people are also obligations.
Scope	A collection of mutual and interrelated obligations for which one manager is responsible (see Section 3.1). NB: although every scope has exactly one manager, a manager can also be responsible for multiple scopes. An example of this is the director of a company who is also the chairman of a football club.

Risk	The assessment made by or on behalf of the manager responsible that a particular obligation may occasionally not be fulfilled or honoured. Examples: • In the case of obligation 1: if the Ministry of Security and Justice estimates that he will not be able to fulfil his 'security of society' obligation. • In the case of obligation 3: an employee of a company believes that he may occasionally not use the telephone made available to him by the company as a good housekeeper (because he sometimes uses it for private calls, for example). Note that another employee at the same company has other types of company resource, who of course uses them differently and therefore has a different risk.
Success	A successful scope (and therefore a successful scope manager) is one where all the obligations for which the manager is responsible (in the scope in question) have been met. In addition, the risks of this remaining so in the future are acceptable to the scope (that is, to the manager of the scope).

NRM helps you answer the following questions:
- Which *obligations* lie at the basis of my success?
- To what degree am I successful?
- What do I contribute towards my own success?
- What *agreements* do I need to make with others in order to be successful?
- What *risks* do I run and how do I manage them?
- How do I adapt my method of working if circumstances make it necessary to do so?

Is anyone else with whom you work also using NRM, and have you decided to share your information with each other? This will make it easier for both parties to work on your success (success governance).

4.2 THE STARTING POINT OF SUCCESS GOVERNANCE: GATHERING BASIC INFORMATION

The first stage of success governance is to set down (once only) what your success consists of. To that end, you make a list in which you set down the following:

1. What results do you want to achieve in order to be able to say that you are successful (we refer to every result as an obligation)?
2. For which party are you achieving these results? This helps you remember to whom you are accountable.
3. According to what criterion can you establish whether the result has been achieved (we refer to a criterion of this kind as a results criterion)? This means that not only do you know where you stand, but also the party to whom you are accountable.

So first – a list of obligations

Because you yourself determine what 'being successful' means for you, it is your task to make the relevant definitions and to set them down. NRM helps you make sure that you continue to be able to achieve the results and obligations on the list and, whenever necessary, to fine-tune them. You yourself determine which results contribute to your success in such a way that it is worth your while to include them on the list.

And then – a list of related expectations

Your success depends on yourself and on others. A company that installs heating boilers depends in part for its success on the company that manufactures the boilers. After all, if they are of poor quality, this can affect the indicators by which the installation company measures its own success, such as reputation, profit, customer satisfaction, or employee satisfaction. This is why it is important that for each of the results you wish to achieve in order to be successful, you are aware of how they depend on the results of others and of other results that you yourself provide. For example, you can only supply (and install) a heating boiler if you have a competent fitter at the place where it is to be installed, the boiler itself, gas, water and electricity supply, items for connecting the boiler to the gas, water and electricity supply, and so on. Some of these items will be arranged by the installation company itself, but will expect others (the gas, water, and electricity supply) to be arranged by another party.

By creating a list of expectations for each obligation, you will gain and maintain a clearer understanding of what you depend on in order to be able to comply with each of your obligations. We define an expectation as a result that you need in order to be able to meet the obligation in question. Expectations in relation to the 'supplying a heating boiler' obligation from the example above are 'the availability of a fitter at the installation location', 'the availability of a heating boiler at the installation location', and so on.

Next – linking expectations to results and assurance criteria

For each of the expectations, you then set down the following:

1. What result are you expecting?
2. Who do you expect to deliver the result (this could be someone else, but also yourself, or 'nature')? This gives you direct information about whom you wish to hold accountable for this.
3. What criterion has to be met before the expected result can be used in order to be able to fulfil the obligation associated with the expectation? This helps you determine whether a result supplied by you or someone else is suitable for your purposes or not. We therefore refer to this as the 'assurance criterion'.

Note: set down the basic information properly

You use the data that you set down as basic information at other times in NRM, for example in coordination with others, dealing with risks, and so on. For this reason, you should set down this data in such a way that it can actually help in these situations. In order for the

result and assurance criteria to be actually used in NRM, they have to meet the following form-related preconditions:

- Every criterion is a tangible result of the obligation and/or expectation, for example a product, a service, or a document. This form-related precondition will ensure that you only carry out tests on things that actually do exist.
- Each criterion sets only unambiguous and measurable requirements of this result. This form-related precondition will ensure that the result is usable for all parties concerned.

An example of a criterion that meets these form-related preconditions is that of 'we deliver every order of heating boilers one week after receipt of the order'. Examples of criteria that do not meet these preconditions are:

- 'The quality has to be good'. This criterion is not concerned with something tangible. We therefore do not know what it can be applied to. The criterion does not contain any measurable requirements either. Even if we knew what it could be applied to, it would not be clear what 'good' quality would actually mean. A tangible criterion could be 'each boiler supplied has no problems at all during its first year of operation'.
- 'Heating boilers must be delivered within one week'. It is just possible to accept that this criterion has a tangible element, namely the supply of heating boilers. However, it does not contain any tangible requirement, because it is not clear from what point the week actually starts. The criterion does meet the form-related preconditions, though, if we also include the time in question: 'heating boilers must be delivered within one week of the date on which the order was sent'.

Briefly: the steps for gathering your basic information

In order to be able to address your concerns about your success, you need a certain amount of basic information, which you gather by setting down the following on paper:

- What obligations collectively define your success? Name them, together with their associated results criteria and the party to whom you are accountable in this regard.
- For each obligation: what expectations do you have in order to be able to honour the obligation?
- For each expectation: on the basis of which criterion do you establish whether a result meets the expectation, and what criterion do you use to decide whether those whom you expect to meet your expectations have done so?

You formulate all the criteria in such a way that they concern tangible results, and you only set requirements of them that are unambiguous and measurable. You are in a position to achieve the obligations that you have entered into. As a result, you are also in a position to specify this basic information about obligations, dependencies, and expectations.

5 NRM STEP BY STEP

The NRM method is not a process in the classical sense in that it prescribes what first needs to happen, and what after that (as is the case in the ISO 31000 standard, for example). The reason for this is that in practice, all kinds of events take place at all kinds of moments, making it necessary to focus attention on risks. Examples of this kind of event include a newspaper report featuring your image, a supplier who goes bankrupt, the discovery of a new way of doing your work, the failure of a system that is critical for your business, and so on. Depending on what the event means for you, this will result in either a lot of work, or not very much.

The NRM method is not just a tool for managing and controlling strategic risks, but also for tactical and operational risks.[16] This requires much more flexible action that is possible with traditional workflows.[17] This flexibility arises because you use the system to signal what work has to be done at any moment. If there are no signals, you do not have to manage anything. If there is one or more signals, then each of them indicates not only the fact that work has to be done, but also what the measurable result of that work should be.

Sections 5.1 to 5.6 cover the activities you can undertake as part of the NRM method. For each activity, we describe what goal it serves, how this is useful for your business, and what the measurable result is when the activity is completed. You should start an activity if you need the results, even if the results criteria have not yet been met, or are no longer being met. If you have already set down the basic information (see Section 4.2), then you have a useful starting point. You then only have to carry out the activities in order to fulfil the results criteria once more.

16 At the time of writing, however, we still need to research the extent to which operational risk management can be made useful in practice. This depends primarily on the nature of the incidents. These are events that require immediate attention in order to prevent a risk from materialising. This means they require immediate action. Additionally, the use of systems can undermine the efficiency that people display in crisis situations.

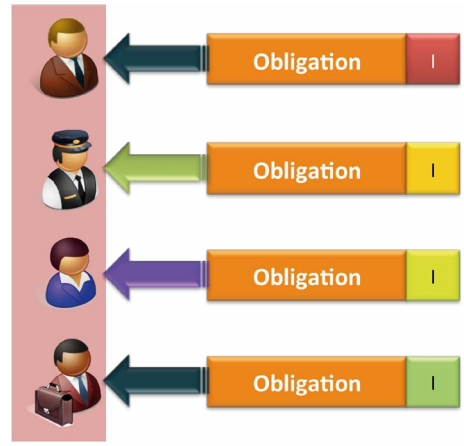
17 In theory, this is possible with workflows. However, they would become so complex it would no longer be possible to keep them complete, consistent, coherent, or up to date.

5.1 BUSINESS IMPACT ASSESSMENT

Your success depends on the degree to which you will be able to meet your obligations. However, the 'value' of an obligation, or the degree to which it contributes towards your success, is not something you determine yourself – it is other people who do that, namely, those towards whom you have the obligation in question and to whom you may be accountable. A good indicator of the value of an obligation (which you can determine yourself) is the amount of damage that you expect to suffer if you fail to comply with or meet the obligation. We refer to this as the 'impact' of the obligation. Making an inventory of your obligations and determining their impact is known as carrying out a Business Impact Assessment (BIA).

An obligation becomes more relevant to you the more it contributes to your success – in other words, the greater the impact of the obligation. You have no interest in actively managing obligations with a low impact (where you suffer no or hardly any damage if you do not fulfil them). After all, they play no or little part in your success. Obligations with a high impact (where you suffer a great deal of damage if you do not fulfil them) do, and that makes them relevant.

If you wish to manage your success, it is important to have an up-to-date BIA list more or less all the time. The list contains all the obligations that are relevant to you, as well as the assessments of their impacts. The illustration here shows this in a diagrammatical form, with the value of the impact shown as a colour (red for high impact, green for a low one). The level of the impact is a measure of the priority that the risk management has in relation to this obligation. An incomplete list, or one that is not up to date, may result in your directing your focus to the wrong areas.



Carrying out a BIA therefore simply amounts to making or updating your BIA list. This is something you do if you feel the need to do so, if you do not yet have a BIA list, for example, or if you believe that it is no longer up to date. An up-to-date BIA list of a scope (at the point when the 'BIA' activity ends) is defined as one that meets the following criteria:

1) The BIA list contains all the obligations whose impact on the scope and related manager is unacceptably high, or could be in the foreseeable future.
2) It is known, for each obligation on the BIA list, to what party the scope manager is accountable in relation to fulfilment of the obligation.

3) For each obligation on the BIA list, the scope manager (or someone acting on his behalf) has made an assessment of the impact.

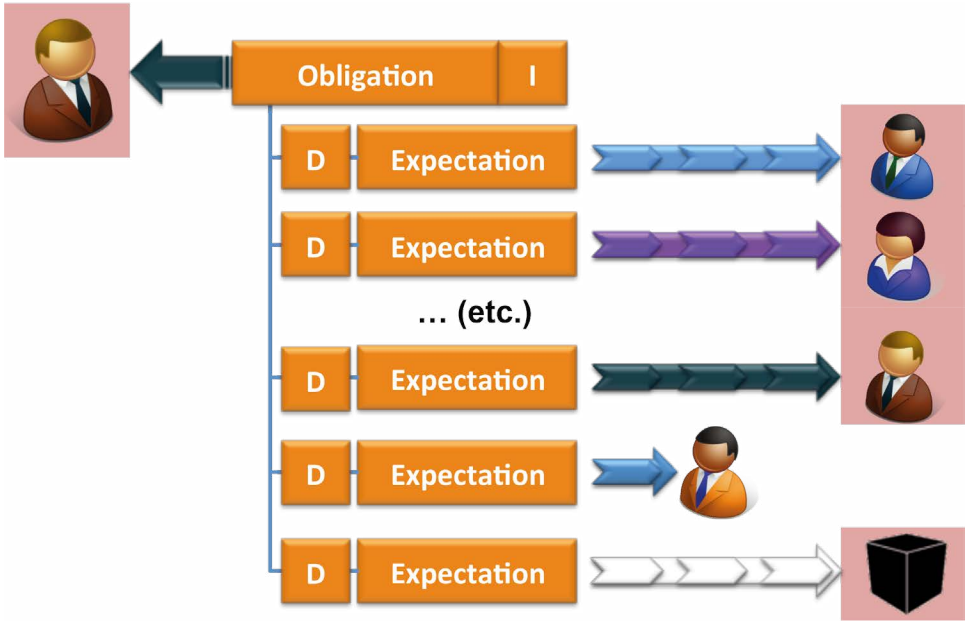
5.2 STRUCTURING THE SCOPE: COVERING OBLIGATIONS

The BIA list contains only obligations that are relevant to your success. That is why it is important that, for each, you are able to establish that they will be fulfilled. To do this, you first need to determine how you are going to do so. This involves structuring your scope.

Fulfilling an obligation is generally just part of your work. Have you committed yourself to delivering all the items ordered with you within one working day? You can arrange this in part yourself (for example, by ordering stocks in good time). However, whether the stocks you have ordered will be delivered to you on time depends on your supplier and the party that organises the transport.

Expectations cover obligation

The illustration here shows that an obligation that you have towards another party is, as it were, 'covered' by a number of expectations that you have of yourself or of others. 'Others' possibly include the person to whom you have the obligation: to fulfil your obligation, you may expect from the same party, for example, that they do something in return. In the example of delivering an order within one working day, it may be that you expect the customer to pay first.



On top of this, you also have special expectations. These are expectations for which nobody is responsible in particular, but which are nonetheless very real. An example is the expectation that the weather will be NRMal on working days (no tsunamis or hurricanes, for example). Expectations of this kind are often those relating to what are referred to as 'acts of God'. This is symbolised in the diagram by the black box.

Another special expectation is one that you set of yourself (symbolised in the diagram by the expectation of the orange figure). NRM assumes that you are congruent, and that implies that if you set an expectation of yourself, you regard it at the same time as an obligation that you should fulfil (for yourself). You can immediately add this obligation to your BIA list and deal with it later, according to how important it is. In the meantime, you can treat it as if it would have been someone else's expectation.

To what extent does your obligation depends on the expectations?

You then need to find out the degree to which fulfilling your obligation depends on the various expectations (symbolised by the 'D' for Dependency in the diagram). After all, whether you are able to deliver an order on time or not will depend more on the expectation of there being sufficient stocks than on the expectation of whether or not tsunamis or hurricanes may occur. You use the 'dependency' to indicate what weighting an expectation has in relation to fulfilling an obligation. The weighting is later used for the purpose of assessing the risk or whether or not you can meet the obligation.

It is important to have a 'cover' for your obligation at more or less any time – in other words, a collection of expectations and 'dependencies' that specify how you wish to fulfil the obligation. This way, you can assess whether, and to what extent, you will meet an expectation (of yourself). You can organise this in different ways, such as by assigning a weighting to each expectation, or by using techniques of the kind mentioned in standards like O-DM[18], or the aforementioned ISO 31000.

We refer to the activities you can use to create or update a cover as 'covering an obligation'. You carry out these activities for each obligation that does not yet have a cover, or whose covers no longer suffice and need updating.

18 The Open Group: Dependency Modeling standard (https://www2.opengroup.org/ogsys/catalog/C133).

Criteria that the cover should meet

A cover of an obligation needs to meet (at the time that the 'set up scope' activity ends) the following criteria:

1) It has been established which single obligation is covered.
2) The cover consists of a possibly empty[19] collection of expectations. This is subject to the following:
   a) If each of the expectations has been sufficiently met, this also means that the obligation has been met.
   b) From the expectations, it has been established that this means that the covered obligation can be fulfilled.
3) For each expectation in this collection, you know from which party you can expect it, or whether it is 'not applicable[20].
4) It has been established how the fulfilment of the obligation depends on each of the expectations, in accordance with the work method for dependencies as laid down for the scope.[21]

In short: when is the setting up of a scope complete?

The activity of setting up the entire scope consists of covering all the obligations on the BIA list. This work is complete when the following criteria have been met:

1) the BIA list of the scope is up to date;
2) all the obligations on the BIA list have been covered.

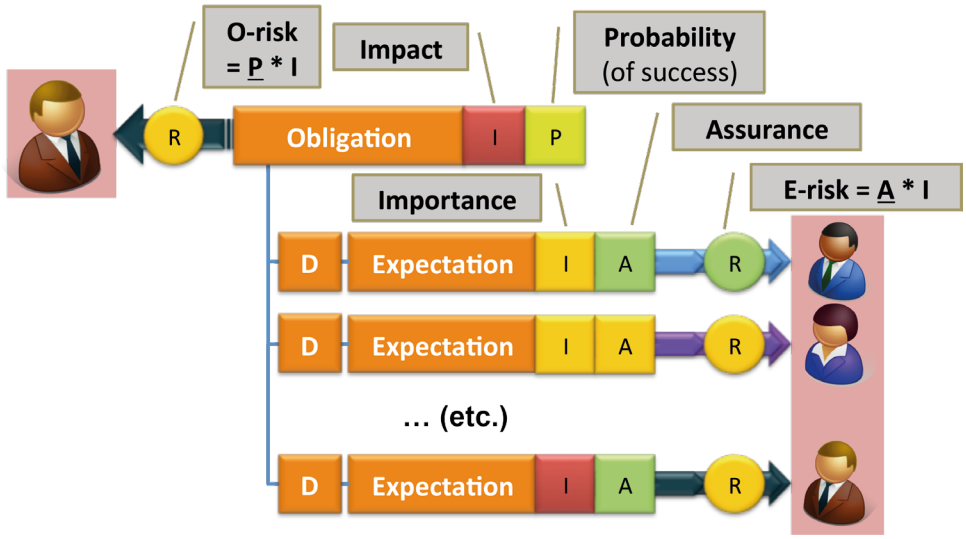
5.3 RISK ASSESSMENT

Risk assessments (RAs) are used to determine the risk of not being able to fulfil an obligation. This is the opposite of determining the probability of being able to fulfil it (probability of success). The risk associated with an obligation (also known as the 'obligation risk' – see Section 3.3) is an important indicator for the scope manager when deciding on which obligation or obligations he should first attend to.

19 If an obligation has a high impact, but is unimportant for the scope manager if it is met, then the cover consists of an empty collection of expectations.

20 This applies among other things to 'acts of God'.

21 In slightly more precise terms: a method needs to be established that can be used to assess the degree to which the obligation will be met. This can be done if an assessment exists for each expectation in the cover of the degree to which the expectation in question will be met (by the person who has the task of fulfilling the expectation).



The above diagram shows the cover of an obligation. The obligation and all the expectations in the cover have been given a number of features, such as 'I' and 'A'. The colours of these features represent their value or significance. Red, for example, means 'this requires attention', while green signifies 'everything is fine'. The features referred to are:

- Impact (of the obligation): the expected amount of damage that will occur for the scope owner if he fails to meet the obligation.
- Importance (of an expectation): the importance of the expectation for the scope, and not just for this obligation, but for every obligation in the scope. This feature is, for expectations, analogous to the impact for obligations: it is an indicator that shows what expectations require greater attention in order to ensure that they are realised (by influencing those who have the task of realising them).
- Assurance (of an expectation): the assessment of the degree of certainty that the scope owner has of the expectation being realised.
- Expectation risk or E-risk[22]: the assessment of the degree to which failure to meet the expectation is a threat to the scope as a whole.
- Probability (of your success): the assessment of the degree to which the obligation is going to be fulfilled. We define 'Probability' (underlined) as the assessment of the degree to which the obligation is not going to be fulfilled. You can assess this quantity (or even calculate it) based on the Assurance (or Assurance) and dependencies D, which we introduced earlier.

22 'E' is derived from 'expectation'. We use 'E-risk' in Dutch, too, as the words for 'expectation' and 'obligation' in that language both begin with the same letter.

- Obligation risk or O-risk[23]: the assessment of the degree to which the obligation is going to be fulfilled.

An RA (for the scope) involves assessing all the expectation risks and the obligation risks in the scope, which you can of course do very easily. In the case of an expectation or obligation for which you need greater substantiation of your assessments, you can use one of the following activities:

RA formula for an expectation

You begin an RA for an expectation if you have not yet determined the risk for it, or if you need to update the risk and have to be able to substantiate it. This is the case if the value of one or more of the features of the expectation (the Importance or the Assurance) has not yet been assessed or if they have been modified. You can formulate the assessment of the expectation risk in the same way as the traditional risk formula (Risk = Probability x Effect). This leads to:

E-risk = Assurance x Importance

In this formula, Assurance (underlined!) stands for the degree of certainty that the scope owner has of the expectation not being realised. Your RA for an expectation is complete once the expectation risk has been calculated according to the formula that you have established in the scope.

RA formula for an obligation

You begin an RA for an obligation if you have not yet determined the risk for it, or if you need to update the risk and have to be able to substantiate it. This is the case if the value of one or more of the features of the obligation (the Impact or the Probability) has not yet been assessed or modified. You can formulate the assessment of the obligation risk in the same way as the traditional risk formula (Risk = Probability x Effect). This leads to:

O-risk = Probability x Impact

In this formula, Probability (underlined!) stands for the degree of certainty that the scope owner has of the obligation not being met. Your RA for an obligation is complete once the obligation risk has been calculated according to the formula that you have established in the scope.

23 'O' is derived from 'obligation'. We use 'O-risk' in Dutch, too, as the words for 'expectation' and 'obligation' in that language both begin with the same letter.

5.4 MATCHING WITH PARTIES WITH WHOM YOU HAVE A RELATIONSHIP

The aim of a relationship between two parties is to enable each other to be successful. Every relationship you enter into is characterised by the obligations and expectations that you have with regard to the other party, and vice versa. Every expectation that you have of another offers them the opportunity to be successful, namely by committing themselves to meet your expectation. Conversely, every obligation that you fulfil for another adds value (makes you successful) – at least, to the extent that the other party appreciates it and expects it of you.

With the 'match relationships' activity, you can manage the obligations and expectations with regard to your various relationships. You do so in such a way that it puts you in a strong position for the purpose of fulfilling your obligations. At the same time, you make it as easy as possible for the other party to meet theirs. In the process, you can and should weigh up various factors in line with your own interests; after all, you yourself are responsible.

Importance of up-to-date list of agenda items

Naturally, you wish to be able to hold effective consultations with your relations (present and future) and that you will help each other be as successful as possible. It is important that the parties discuss with each other every subject that is relevant to that context. You can do this, for example, by maintaining a list of agenda items for a relation. This will enable you to decide to schedule a meeting at any time, and to estimate how much time will be needed for it. Agenda items result from various activities. Two examples:

- With the 'treating risk' activity, you decide how a particular risk should be treated. It may be necessary to consult with the relations concerned before that decision is taken. A similar 'risk issue' is then added to the list of agenda items for these relations. You then defer the decision on how to treat the risk in order to create an opportunity to hold consultations.
- With the 'matching expectations and obligations' activity, you check whether there are sufficient similarities between your relations and yourself with regard to your mutual obligations and expectations. This activity may reveal issues that need to be harmonised. You then add them to the list of agenda items.

Agenda items should lead to a decision

In principle, every activity can make additions to the list of agenda items, as long it is clear to where discussion of an agenda item could or should lead. Discussion of any agenda item should in principle lead to one or more decisions, such as ending, altering, or creating expectations or obligations with regard to the party with whom you have held the discussion, or to a decision on how you wish to treat a risk, or to assessing or re-assessing the impact or assurance (which itself will affect the risk assessments).

The decisions and conclusions that you reach as a result of these discussions could have potentially major consequences, both for you and your relations. That is why it is important to be able to set every major issue on the agenda, and to know for each agenda item why they should be discussed, and which of the consequences you will have to opt for.

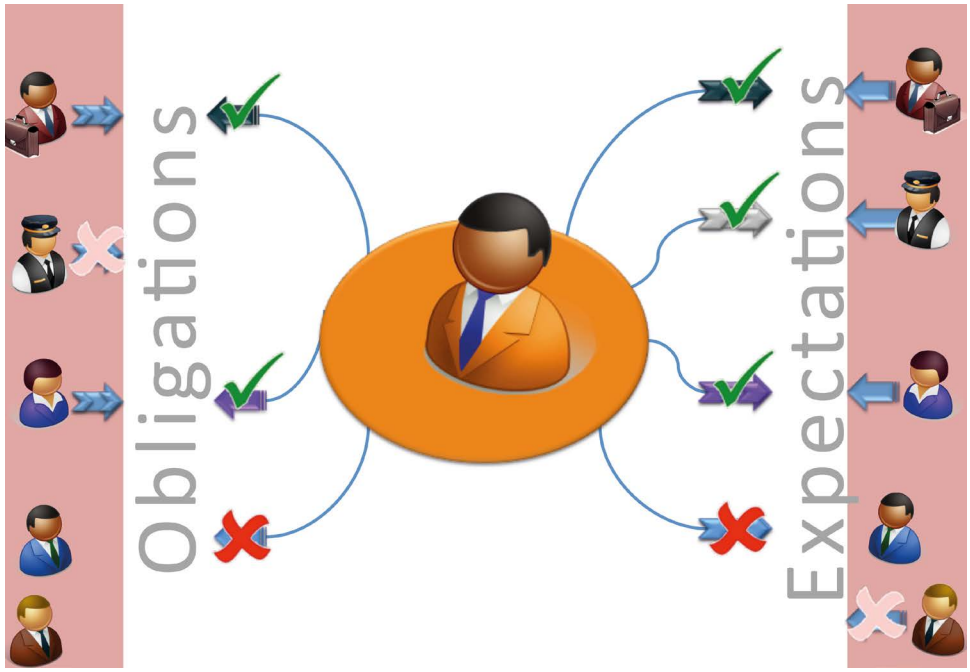
When does the 'match with relation' activity start?

You begin the 'match with relation' activity when there are agenda items on the list of agenda items for discussions with a relation. The activity is complete once the list is empty. Note that it is highly likely (and permissible) that the list of agenda items will be modified while the activity is being carried out. For example, agenda items may disappear as a result of the decisions you take. Two examples:

- If you have an obligation to another party for which he has no corresponding expectation (see Section 5.5), and you decide to remove the obligation (from your BIA list). In that case, the agenda item disappears.
- If you read in the newspaper that your relation is trying to defraud his relations, then this reduces the assurance of expectations that you have of the relation in question. This leads to a change of expectation risks (see Section 5.3) and are possible risks that need to be treated (see Section 5.6).

5.5 MATCHING OBLIGATIONS AND EXPECTATIONS

Parties that match themselves enable each other to realise their obligations as efficiently and effectively as possible. This is done within the limitations that are part and parcel of relationships. Parties are matched if each knows what mutual obligations the other has, and if they both expect that these obligations will be met. We refer to this activity as 'matching obligations and expectations'.



In the following cases, there is a mismatch with a party:

1) If you expect something of a party, but are not sufficiently sure that that party is going to meet that expectation, or if you are not sufficiently sure whether or not that party has an obligation towards you in order to meet your expectation. For example, if you expect your order to be delivered within one working day, while the supplier does not feel obliged to do so, you may have a problem.
2) If you have or feel an obligation towards that party, while you are insufficiently sure that that party has an expectation of you that you could meet this obligation. In essence, you have committed yourself to carrying out work that will not be appreciated and therefore will not contribute to your success.

How the mismatches relate to the other activities

It is important that you have an up-to-date list of matching issues at more or less any time for each of the parties towards whom you have one or more obligations or expectations. It is only then that you can establish whether, and to what extent, a matching issue could become a problem. You can then determine how you will deal with the issue. The list can form part[24] of the agenda for a discussion with the party in question. A discussion of this kind may lead to the creation, modification, or removal of obligations or expectations, which itself may lead to alterations to the BIA list, covers, and the like.

24 If this party also uses NRM, its list of issues regarding you will also be added to the agenda.

5.6 TREATING RISKS

In NRM, risks (both obligation and expectation risks) are indicators that require the attention of management. The scale of the risk of an obligation or expectation is the strength of the priority with which the obligation or expectation requires your attention. A major obligation risk suggests to you that you are probably not only not sufficiently well placed in order to fulfil the obligation, but also that this will leave you with a loss that you would like to prevent, if possible. A major expectation risk suggests that the party may not meet the expectation to the required degree, even though this is important to you, given the obligations that depend upon it.

An overview of every relevant risk, thanks to NRM

As in traditional risk management, major risks require a decision from which it becomes clear how you prefer to deal with this risk (referred to as 'risk treatment'[25]). These decisions are generally classified as the mitigation, transfer, avoidance, or acceptance of risks. In many cases, however, it will be a combination of options. In order to be able to meet your 'good housekeeping' obligation, you may have an expectation that nothing will be stolen. If this expectation is important for you and if it has a low level of assurance, you may decide to improve fencing, for example (a mitigating measure) and to take out anti-theft insurance (transfer of the risk). We can see from this example the problem of risk management – decisions you take affect not just the risk that was requiring your attention, but possibly also other risks. Taking out insurance costs money, for example, and if you have an obligation that says your outgoings may not exceed your revenue, then the risk of this obligation is greater than would be the case if you did not take out insurance. With NRM, you can show exactly what needs to be done to gain and keep a complete, consistent, coherent, and up-to-date overview of all the risks that are relevant to you.

Possible decisions on a risk

With NRM, you can treat a risk in the following ways (the risk treatment decision for the risk concerned):

1) You accept the risk (as in traditional risk management) for what it is.
2) You put the 'risk issue' on the list of agenda items that you maintain for the relation towards whom you have the obligation or expectation associated with the risk, and discuss it with him (see Section 5.4).
3) You amend or remove the obligation or expectation (comparable with the traditional transfer or avoidance of risks). You ensure that you have less or nothing more to do with the obligation concerned, as a result of which you reduce the associated risk. Similarly, if you expect less from the other party, the associated expectation risk will be reduced. However, this could increase the risks for the obligations in whose cover the expectation is located.

25 See ISO/IEC FDIS 27005 – Information technology – Security techniques – Information security risk management

4) You create obligations (primarily for yourself) and/or expectations (of yourself or of others). You are hereby specifying your 'measures' aimed at increasing the assurance that the original obligation or expectation will be fulfilled. This is comparable to the traditional 'mitigation' of risks.

When does the 'treating a risk' activity begin?

You begin the 'treating a risk' activity for each risk:

1. whose value has been assessed in an RA at a particular time; and
2. whose value has not been assessed at a later time; and
3. whose assessed value is greater than the threshold value for this that has been laid down within the scope; and
4. for which no risk treatment decision has been taken that refers to the RA meant under 1 or the value meant under 2.

When does the 'treating a risk' activity end?

The activity ends as soon as a new RA has been done for the risk in question, or if a risk treatment decision has been taken with which you amend or remove the obligation or expectation.

Note that every change of value of impact, assurance, and so on can lead to new risk treatment decisions. If you notice that this requires a needless amount of your attention, you may decide within your scope that 'medium risks', for example, should be treated in one standard manner, such as by placing them on the relevant list of agenda items. You may also decide to increase the threshold value slightly.

5.7 SUMMARY OF THE METHOD

Implementing the NRM process in your scope means having an overview of your obligations and associated risks at any time that is complete, consistent and up to date in a way that puts you in a position to take immediate action as soon as a risk becomes unacceptably large. For an overview of these risks, you need an overview of your expectations, the assurance that you have of them, and the dependencies between obligations and expectations.

When you set up the NRM process in a scope, you make explicit both the obligations and expectations in the scope, and how they are interrelated. For each obligation, you also determine their impact, and for each expectation, the degree of assurance you have that the expectation will be realised. You can use this as the basis for assessing the various expectation and obligation risks.

A number of criteria[26] have to be met before you can establish whether the overview of the obligations and their associated risks is sufficiently complete, consistent and up to date. If any criterion is not met, you will have to start a task aimed at fulfilling the criterion in question.

Risk management is a knowledge-intensive process. Generally speaking, processes of this kind cannot be adequately described using classic process technology, such as workflows. For this reason, NRM does not show the sequence in which tasks should be carried out – instead, it restricts itself to indicating the results that need to be achieved. Nor does NRM state how you should achieve these results. A consequence of this is that you can use the methods mentioned in the standards in NRM as well. This applies for example to the methods for risk analysis that are mentioned in ISO 31000.

NRM lets the scope manager decide what results he needs, how high a priority they have, and what resources he deploys to achieve them. If the scope manager responds immediately to every signal by carrying out the task concerned, then he will be managing his risks in real-time, more or less. If risk management tasks are performed periodically (every quarter, for example), then the implementation method will more closely resemble a traditional approach to risk management. The optimum working method will vary from one manager (or scope manager) to another. Everyone is free to apply their own working method as they see fit.

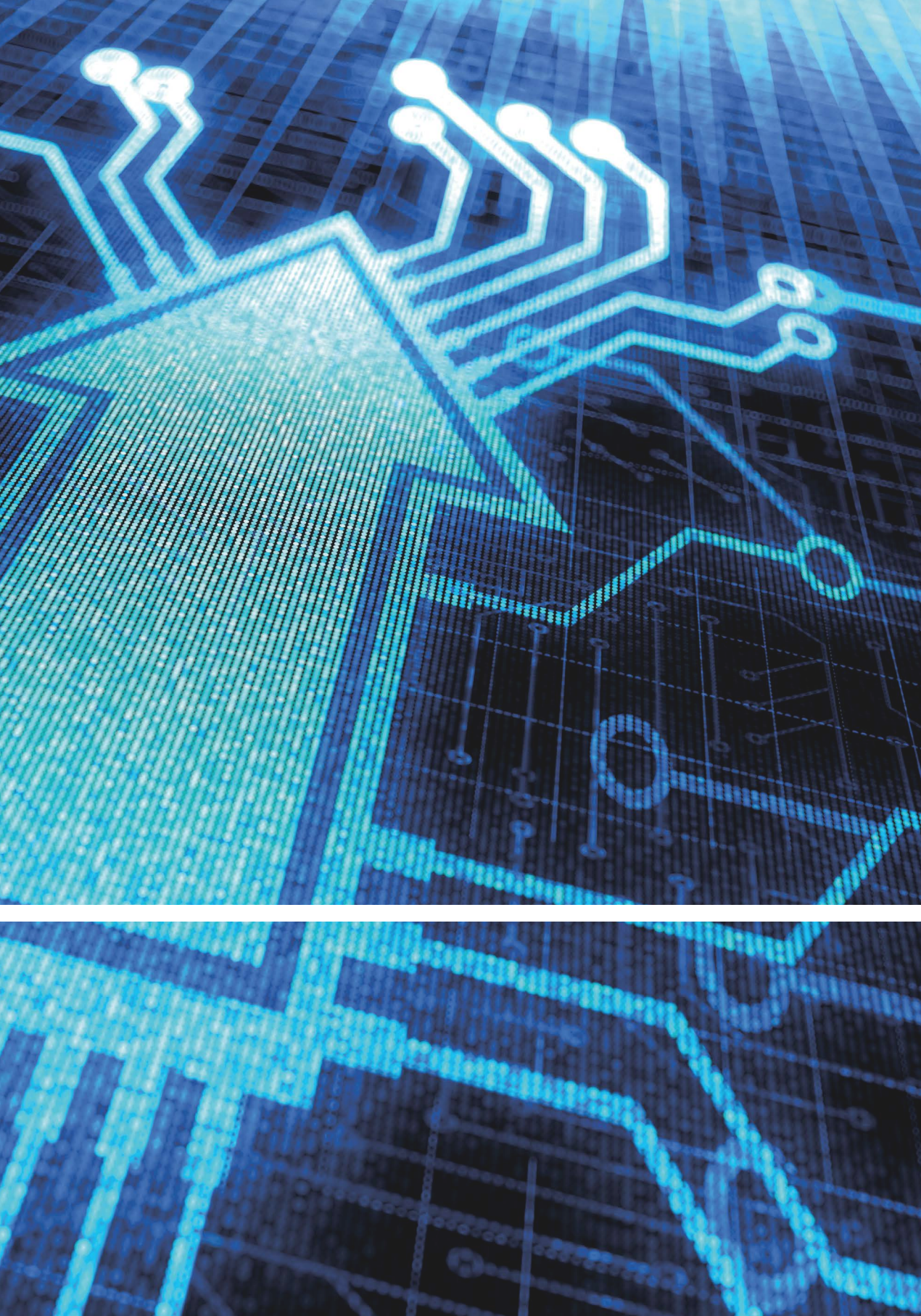
26 These concern not just the obligations and obligation risks, but also matters derived from them, such as the expectations, assurance, dependence of obligations on expectations, etc.

An overview of the method

In the table below, we show the criteria that a complete, consistent, and up-to-date overview of obligations, obligation risks, and the remaining matters, should meet.

ACTIVITY	RESULT TO BE ACHIEVED
Introduction of NRM	No more NRM work is needed in a scope, if the scope meets each of the following criteria: 1. Every obligation risk has been assessed ('assess obligation risk' activity). 2. Every obligation risk is acceptable, or the scope manager has taken a decision that the mutual interrelationships between all the obligation risks in his scope are acceptable.
Business Impact Assessment (BIA)	An up-to-date BIA list of a scope should meet each of the following criteria: 1. The BIA list contains all the obligations of the scope whose impact for the scope manager is unacceptably high, or could be in the foreseeable future. 2. For each obligation on the BIA list, the identity is known of the party to whom the party responsible for fulfilling the obligation in question is accountable. 3. For each obligation on the BIA list, the impact has been assessed by, or on behalf of, the scope manager. 4. It has been decided by, or on behalf of, the scope manager, that the BIA list meets the preceding results criteria. 5. There are no known suspicions, reasons, or any other triggers in the scope on the basis of which the aforementioned decision would need to be reviewed.
Set up scope	A scope that has been set up should meet the following criteria: 1. There is an up-to-date BIA list ('BIA' activity). 2. Every obligation on the BIA list is covered.
Covering obligation	An obligation is covered if it meets each of the following criteria: 1. There is at least one (possible empty) collection of expectations that, were they to be realised (to a sufficient degree), then the obligation will have been met. 2. It has been determined that this collection will be used in order to meet the obligation (this makes the collection a cover).
Keeping track of issues	An up-to-date list of issues of a scope of a particular party should meet each of the following criteria: 1. The list of issues contains all the issues of the scope of the party concerned that the scope manager would like to see addressed. 2. The list of issues contains all the obligations of the scope towards the party concerned, about which it is not known what expectation the other party has towards them. 3. The list of issues contains all the expectations of the scope of the party concerned, about which it is not known what obligation the other party has towards them. 4. The list of issues contains all the assurance criteria for which data or reports from the party concerned are needed, and for which no expectation on the part of that party exists with regard to their delivery. 5. There are no known suspicions, reasons, or any other triggers in the scope on the basis of which the list of issues should be updated.

ACTIVITY	RESULT TO BE ACHIEVED
Making agreements	An up-to-date contract between a scope and another party should meet each of the following criteria: 1. The contract contains all the obligations within the scope towards the party concerned, and the expectations of that party correspond to these obligations. 2. For each of these obligations, the contract contains a results criterion on the basis of which both parties are able to establish without question whether or not the obligation has been met. 3. The contract also contains all the expectations that are expected within the scope of the party concerned, and the obligations of the party correspond to them. 4. For each of these expectations, the contract contains an assurance criterion on the basis of which both parties are able to establish without question whether or not the expectation has been met. 5. The contract contains reporting criteria on the basis of which it can be established what must be reported by the scope manager to the other party, how this should be done, and how frequently. 6. The contract contains reporting criteria on the basis of which it can be established what must be reported by the other party to the scope manager, how this should be done, and how frequently. 7. Every issue on the list of issues of the scope with regard to the other party has been addressed by the contract. 8. The other party has committed itself to the contract (for example, by placing a signature, digital or otherwise). 9. There are no known suspicions, reasons, or any other triggers in the scope on the basis of which the contract should be reviewed.
Contract management	A scope, all of whose contracts are managed, meets the 'list of issues for all relations (parties towards which the scope has obligations, expectations, or issues) being empty' criterion.
Assessing obligation risks	A scope for which every obligation risk has been assessed should meet each of the following criteria: 1. The scope has been set up ('set up scope' activity). 2. The expectation risk for each expectation in the cover of an obligation that appears on the BIA list has been assessed ('assess expectation risks' activity). 3. For each obligation that appears on the BIA list, the obligation risk has been assessed on the basis of data from the BAA list for the expectations that form the cover of the obligation.



APPENDIX – TERMINOLOGY

TERM		DESCRIPTION
Activity	on an *object*	The specification of a package of work that can be carried out on aspects of the object concerned.
Cover	of an *obligation*	A collection of expectations with which the scope manager has determined that the obligation (of the cover) will be fulfilled.
Dependency coefficient	between an *expectation* and an *obligation*	The degree to which non-realisation of the expectation results in the relevant obligation not being met either.
BAA list	of a *scope*	A list of all the expectations of the scope, the uncertainty of which is unacceptably high for the scope manager, or could be in the foreseeable future.
BIA list	of a *scope*	A list of all the obligations of the scope, the impact of which is unacceptably high for the scope manager, or could be in the foreseeable future.
Contract	between a *manager* and another *party*	A collection of obligations and expectations by the manager with regard to the other party, to which both the scope manager and the other party have committed themselves.
Criterion		A verifiable, logical expression, on the basis of which an unambiguous judgement can be made.
Impact	of an *obligation*	An assessment of the seriousness of the damage that will occur if the obligation is not met. This is done by, or on behalf of, the scope manager with responsibility for fulfilment of the obligation.
List of issues	of a *scope*, in relation to a *party*	A list of matters that are important to the scope (or scope manager) for the purpose of discussion with the other party.
Manager	of a *scope*	A person, or a group of persons, who can be held to account if any obligation of the scope has not been, or cannot be, fulfilled.
Mission	of a *scope*	The obligation of the scope in question (towards itself) that describes the reasons for the scope's existence.
Object		A cohesive quantity of data that correspond to the specifications of type (or category) of object.

TERM		DESCRIPTION
Uncertainty	of an *expectation*	An assessment of the degree to which it is expected that the expectation will be realised. This is done by, or on behalf of, the scope manager who set the expectation.
Party		A person, group of persons, or organisation who can be held accountable.
Post-condition	of an *activity*	The collection of conditions (criteria) that all have to be fulfilled by performing the activity.
Precondition	of an *activity*	The collection of conditions (criteria) that all have to be in place before a new activity can be started.
Secondary condition	of an *activity*	The collection of conditions (criteria) that all have to be in place during the execution of every aspect of the activity.
Results criterion	of an *obligation*	A criterion that serves to make it possible to determine unambiguously whether the associated obligation has been met.
Obligation risk	of an *obligation*	The assessment of the degree to which this obligation will not be fulfilled. This is done by, or on behalf of, the manager responsible (for the obligation).
Expectation risk	of an *expectation*	The assessment of the degree to which this expectation will not be realised. This is done by, or on behalf of, the manager responsible (for the expectation).
Scope		A space in which a manager is responsible for fulfilling a number of interrelated obligations.
Success	of a *scope*	The degree to which all the obligations in a scope are fulfilled, or that all associated risks are acceptable to the scope manager, either individually or collectively.
Trigger	of an *activity*	The collection of conditions (criteria) that starting an aspect of the activity in question causes.
Obligation	of a *scope* towards a *party*	Something that can be fulfilled within the scope; the scope manager is accountable for this (and suffers 'pain' if this does not happen).
Expectation	of a *scope* towards a *party*	Something that the manager of the scope expects the party to be able to realise (for fulfilling at least one of his obligations).
Expectation criterion	of an *expectation*	A criterion that serves to make it possible to determine unambiguously whether the associated expectation has been met.
Collection of expectations	of an *obligation*	A collection of expectations that makes it potentially possible to meet the obligation (if the expectations were to be realised to a sufficient degree).
Assurance criterion	of an *expectation*	The criterion on the basis of which it is possible to distinguish whether, and to what extent, the associated expectation is going to be realised by the party that is expected to do so.

As organizations and systems become increasingly complex, dynamic, and networked, it also becomes increasingly difficult to identify, assess and manage the associated risks. The risk management process itself is at risk. Current methods have difficulties producing sufficiently complete, coherent, consistent and current risk overviews in a timely manner using an acceptable amount of resources. To address such risks, a new way of thinking about risks and risk management is needed to ensure that any risk management activity:

- Is only executed if the produced result actually contributes to risk management (i.e.: it must have business relevance, and this should be very explicit).
- Is sufficiently small and manageable for the person that executes it, minimizing errors and time consumption.

Such properties guarantee that no unnecessary work is done, and that the work is being done effectively while minimizing effort.

Networked Risk Management (NRM) is a new risk management concept and methodology that has the aforementioned properties. Activities within the NRM process, e.g. for assessing risks, may be executed using existing methodologies, and can be used in combination with standards such as ISO 27000 (27005) and ISO 31000 (31010).

NRM helps you answer the following questions:

- Which obligations lie at the basis of my success?
- To what degree am I successful – what are my risks?
- What do I contribute towards my own success?
- What agreements do I need to make with others in order to be successful?
- What risks do I run and how do I manage them?
- How do I adapt my method of working if circumstances make it necessary to do so?

The authors work for the applied research organisation TNO and are de developers of the NRM methodology. We wish you success with the application of the NRM mind-set and methodology in making your organisation more secure and better prepared for our fast changing networked world.