

2015

## Risk management 2.0: From risk-aware to risk-based in a political-administrative context; executive summary

Research on risk management at the Directorate-General Police, Ministry of Security and Justice



Irna van der Molen

1 September 2015

## Scientific Committee University of Twente:

Prof. Dr. Ir. J.I.M. Halman

Dr. Ir. M. van Staveren

### *External:*

Frederik Jansen, MPM.

### *Contact person:*

Dr. Irna van der Molen, Coordinator Centre for Risk Management, Safety and Security

University of Twente, PO Box 217, 7500 AE Enschede

Telephone: +31-53 4893542 / email: p.vandermolen@utwente.nl

## **Colofon**

Scientific Research and Documentation Centre (WODC)

Department of External Scientific Relations (EWB)

Turfmarkt 147

2511 DJ Den Haag

PO Box 20301

2500 EH The Hague

[www.wodc.nl](http://www.wodc.nl)

© WODC, Ministry of Security and Justice. Copyrights reserved.

## SUMMARY AND CONCLUSIONS

### BACKGROUND

With the establishment of a National Police organization, the Dutch government intends to work towards a more uniform approach in the administration, implementation and management of the police in the Netherlands. In this context, the objectives are to achieve a higher effectiveness, a reduction of the administrative burden and operating costs, and more unity and transparency in the management, without compromising on the quality of police work at local level (Wetenschappelijk Onderzoek- en Documentatiecentrum, WODC, 2014). The Directorate-General Police (DGPoI), that is part of the Ministry of Security and Justice, seeks to achieve optimization of the police force; to arrive at a police-organization that is well equipped; and to increase the visibility of the performance of the police (Van Aalst, Laan and Van Veen, Position Paper, 2014). This requires, however, a well-functioning risk management system. For that reason, the University of Twente has carried out research, commissioned by the Scientific Research and Documentation Centre (WODC). The outcome of this research, aims to contribute to a more effective risk management system of DGPoI, aligned with the characteristics and routine of the organization.

The usefulness and necessity of a well-functioning risk management system was repeatedly confirmed by reports in the traditional and social media (such as the news reports on the delays and exceeding budgets for the establishment of the National Police), by questions of members of Parliament (e.g. questions related to a settlement with former drug offender Cees H.) or by commotion in the streets (riots in the 'Schilderswijk' that emerged shortly after the death of Mitch Henriquez, July 2015). Communication experts refer to these events as 'mediatized incidents': incidents that receive significant media attention, which is then followed by a public outcry; and by an intensive accountability process in which the responsible minister is under great pressure to answer questions or take action.

In accordance with the guidelines for risk management at the Ministry of Security and Justice, a *risk* is defined here, as "an uncertain event that can result in deviation from the set objectives and requirements" (Ministerie van Veiligheid en Justitie, 2014, p. 16). *Risk management* is defined by the Ministry of Security and Justice as "the totality of activities and measures to address and manage risks in an explicit and systemic way" (Ministerie van Veiligheid en Justitie, 2014, p. 17). The *risk management process* consists, according to the inception report, of "systemic application of management policy, procedures and routines regarding the activities of communication, consultation and mapping the context, identification, analysis, evaluating, treatment, monitoring and reviewing the risks" (WODC, 2014, p. 3).

### RESEARCH QUESTIONS

The research objective is to create an overview of relevant risk management standards and frameworks currently available, which can be applied by DGPoI, and which is aligned to the tasks, characteristics and specific needs of DGPoI. This includes both the 'hard' side of risk management, with attention for planning, control, systems and manageability; and the 'soft' side of risk management, i.e. a risk-based approach, with an emphasis on the role of the human being, culture, the importance of flexibility, adaptation and learning, and the awareness that organizations can only be engineered to a certain extent (translated and adapted from Van Staveren, 2015, p. 81). The first question, as formulated by the WODC, is:

- A. *What is the standard or framework (or combination thereof) for risk management, that can be applied by DGPoI and fits best with the specific tasks and characteristics of DGPoI, the specific needs with regard to risk management, in particular the relation to the political-administrative context of DGPoI in which she operates?*

The 'best fit' is operationalized based on (a) the specific tasks and characteristics of DGPol as expressed in the document stating DGPol's ambitions and the papers on a risk-oriented approach ['Risicogeorienteerd werken']; and (b) the specific needs as expressed by staff members during interviews. We formulated the following sub-questions<sup>1</sup>:

1. How is risk management defined in the scientific literature? (chapter 2);
2. Which insights follow from the scientific debate? (chapter 3);
3. Which standard or framework has the best 'fit' for application by DGPol? (chapter 4).

- B. *How can the selected standard or framework be embedded in the structure, work processes and reporting of DGPol in such a way that it is aligned with the specific tasks and characteristics of DGPol and the specific needs with regard to risk management, in particular in relation to the political-administrative context of DGPol?*<sup>2</sup>

This second question can be further divided in the following sub-questions:

1. How is risk management currently structured at DGPol? (chapter 5);
2. How can the selected standard or framework be combined with the praxis of DGPol? (chapter 6);
3. How can risk in the political-administrative context be easier recognized? (chapter 6).

The combination of answers to these questions will result to the answers on Questions A and B in chapter 6.

The 'hard' side of risk management - also referred to in this report as conventional or traditional risk management - positions the system and methods at the core of risk management, while the 'soft' side of risk management is guided by objectives and principles, and allows for flexibility in the methods and a variety of instruments chosen. Since the nature of these two approaches is very different, both approaches will be studied in terms of their fit with the organization. The conventional approach is at the center-stage of the first part of this report (chapter 1-3), and includes an inventory of the frameworks and standards that are best known and most in use in the Netherlands. The 'soft' side of risk management is discussed in the second part of this report. In chapter 5 and 6, the design of risk management, we propose a combination of 'hard' and 'soft' risk management, that is aligned as much as possible with the specific tasks, characteristics and needs of DGPol. We refer to this as a risk-driven<sup>3</sup> and future-oriented risk management approach.

## METHODS

Literature distinguishes, on the one hand, between fundamental research (theory-developing or theory-testing) and applied research (problem signaling, diagnostic, design oriented, change oriented, or evaluative research) (Verschuren en Doorewaard, 2005, pp. 26-35); and on the other hand between quantitative and qualitative research. The analysis and diagnosis in this research are largely based on applied qualitative research.

The first part of this research is descriptive and exploratory in nature. Sub-questions 1 and 2 are mostly conceptual and theoretical in nature. Risk management and the 'risk-driven' approach are related to insights from various scientific disciplines. This is referred to as 'theory informed field problem solving' (Van Aken, Berends, and Van der Bij, 2012, p. 28). For question 3, we conducted literature research, collected and analyzed documents and conducted

---

<sup>1</sup> The sub-questions are again subdivided (in a, b, c, d) in the chapters.

<sup>2</sup> Based on structured research and careful scrutiny, the researchers provide DGPol with a direction, instruments, and a principles-based framework for action. Further development of instruments or methods falls outside the scope of this research assignment.

<sup>3</sup> 'Risicogestuurd werken' is translated in this document as a 'risk-based approach'.

structured interviews. The second part (with sub-questions 4, 5 and 6) is also based on applied research. For this, we followed the first three steps of the Problem Solving Cycle, including the problem definition, analysis and diagnosis of the current situation; to arrive at suggestions for future risk management. A pilot intervention and an evaluation based on such an intervention were not possible within the time available for the research. During the entire course of the research project, we applied the following methods: literature research, document analysis, interviews and a media analysis.

---

## LITERATURE RESEARCH

The problem definition refers to several core concepts, in particular: ‘risk management’, ‘sense and respond’, the ‘political-administrative context’, ‘public accountability’, ‘stakeholder management’, and the ‘learning organization’. These concepts served as the basis for the search for scientific literature (Verschuren and Doorewaard, 2005, p. 54; Van Aken, Berends and Van der Bij, 2012, p. 83). By positioning the core concepts in the literature, as shown in table 1.1, we were able to identify the necessary points of departure for the further design.

---

## DOCUMENT ANALYSIS

During the research, the research team has collected policy papers, reports, annual reports, letters to the Parliament, manuals, visions, position papers, development plans, a document with ambitions, management plans, realization plans, investigation reports from the Inspection Security and Justice, responses from the Minister to these reports, legislation, parliamentary inquiry reports, and policy guidelines. The selection and analysis was based on an assessment regarding the relevance for answering the questions and sub-questions.

---

## STRUCTURED INTERVIEWS

The first round of interviews (structured interviews) served to get a representative overview of the standards, frameworks and instruments used within DGPol, and of the perceptions with regard to the advantages and disadvantages and criteria for further testing. The questionnaires included a combination of open and closed questions. The interviews are based on a select sample (n=14 in 12 interviews); by means of purposive judgement sampling (Cooper and Schindler, 2011, p. 385). The interview protocols and an overview of respondents can be found in the Annexes.

---

## IN-DEPTH INTERVIEWS

The questions in the second round of interviews (in-depth interviews) were tailored to the respondents’ former and current position, and their administrative, managerial or professional experience. Similar to the first round, the interviews were based on a select sample (n=10 in 8 interviews), by means of purposive judgement sampling (Cooper and Schindler, 2011, p. 385), in combination with snowball sampling (Cooper and Schindler, 2011, p. 386). The selection of respondents was facilitated by contact persons from DGPol, through members of the scientific supervision committee, the WODC and others during the research. An overview of respondents can be found in the annexes.

---

## MEDIA ANALYSIS

Between 18 February and 31 March, DGPol sent a digital collection of newspaper cuttings to the researcher, which were then analyzed. For this purpose, we used the content analysis method as first applied by Semetko and Valkenburg (2000). An and Gower (2009) used the same frames of Semetko and Valkenburg (2000) and studied how media frame crises. Their article reveals a thematic relevance to the research on risk management for DGPol.

Although risk management is not always related to crisis situations; it does relate to uncertain events and incidents that can play a major role in the news reporting; and which can – similar to crises – have an impact on the legitimacy of the organization, the functioning of the organization and the achievement of objectives.

## FINDINGS

### HOW ARE RISK AND RISK MANAGEMENT DEFINED IN SCIENTIFIC LITERATURE?

Risk management has gained momentum in the public sector from the 1990s onwards, partly influenced by New Public Management and the rising demand for accountability. Risk Management provides input to satisfy the demand for accountability, but at the same time, it has not always been successful in preventing incidents or institutional failures. Recent scientific literature emphasize that the current risk management practices do not sufficiently take uncertainties into account. Risk Management is defined as: “the totality of activities and measures to address and manage risks in an explicit and systemic way” (translated from: Ministerie van Veiligheid en Justitie, 2014, p. 17) or as the “purposeful, explicit, structured, communicative and continuous dealing with risks” (Van Staveren, 2015, p. 60).

Risks are often defined in terms of the probability or possibility that something happens, times the adverse effect once it happens (‘probability times effect’), or variations thereof. The literature research reveals that this definition is strongly criticized, for several reasons. The most important conclusion is that this generally used definition is not applicable to risks “that are characterized by high levels of complexity; uncertainty and ambiguity<sup>4</sup>” (Renn, Klinke and Van Asselt, 2011, p. 234). Many of the risks that DGPoI has to deal with at a program and strategic level, have such characteristics.

Complex transition processes, such as the strategic plan for Information and Communication Technology (ICT) of the National Police [‘Aanvalsplan ICT Nationale Politie’], the centralized control room [‘Nationale Meldkamer’], and the action program to reduce the number of rules and increase the presence of the police on the streets [‘Minder regels, Meer op Straat’], are examples of such programs that are characterized by complexity, uncertainty and ambiguity. Moreover, these involve technological innovations. Depending on the levels and nature of complexity, uncertainty and ambiguity, different strategies are required, and particular tools can be selected, whether or not in combination with stakeholder management. This research provides three alternatives to deal with this:

1. Application of the Risk Diagnosing Methodology in case of (radical) innovation and transition processes. In their analysis of risks in ‘radical’ innovation projects, Keizer and Halman (2009) and Keizer, Halman and Song (2002) suggest a methodology to determine the risks in radical innovation processes, identifying the uncertainties, the extent to which risks can be influenced, and the interests that play a role. Although this methodology is originally developed for technical innovation processes, it can also be applied to complex transition processes.
2. Application of the precautionary principle in case of major uncertainties. The way in which the precautionary principle can be applied, is discussed in chapter 2.4.
3. Application of a combined ‘Risk Governance Approach’ and stakeholder management strategy, in case of multi-stakeholder and multi-level decision making, when stakeholders are involved from their own perspective, with their own interests, expertise, objectives and activities. This approach transcends the level

---

<sup>4</sup> These concepts are further elaborated upon in chapter 2.

of the organization itself. The more the complexity increases to govern or manage a program, a strategy or a process, the more suitable is application of a risk governance approach (Renn Klinke and Van Asselt, 2011). A good stakeholder analysis and combination with the stakeholder management strategy are indispensable for an effective application of the risk governance approach.

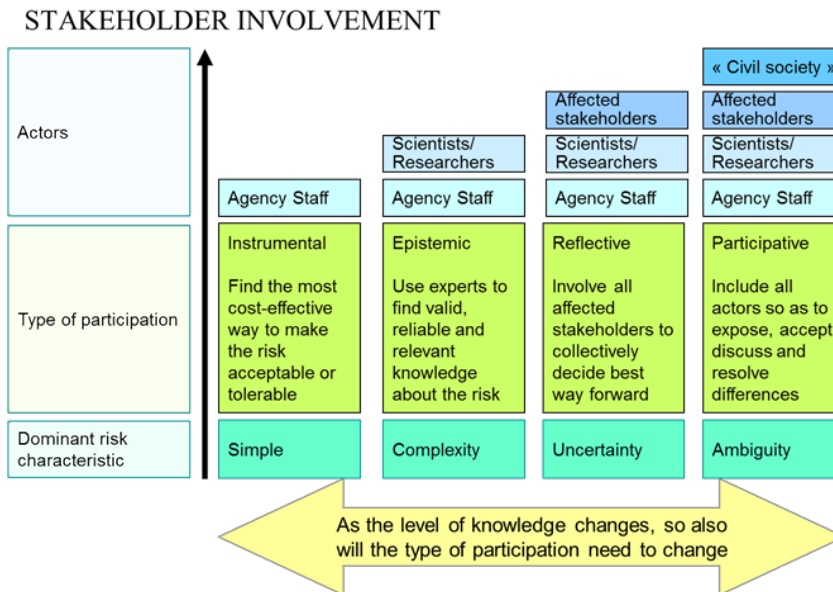


Figure SC1: Stakeholder participation according to the Risk Governance approach. Source: Renn (2007)

#### WHICH APPROACH IS SUITABLE FOR DGPOL?

Four general approaches can be distinguished in the scientific literature, i.e.: (1) scientific risk management that is informed by quantitative models and an instrumentalist approach – in this report referred to as ‘traditional or conventional risk management’ (elements of this are clearly visible in the Plan and Control Cycle), (2) heuristic risk management, based on intuitive decision making, experience and incremental learning (all present at DGPOL), (3) fatalistic or reactive risk management, where only then action is taken when this is required by law or regulations, and (4) holistic risk management that looks at future developments, anticipates to future risks, and takes preventive measures (Van Staveren, 2009, Smalman en Weir, 1999). Within DGPOL we identified a combination of the first two approaches: risk management informed by dashboard methods; where risk is defined as the probability times the adverse effect and the approach following from this; and intuitive risk management which is applied in particular to risks in terms of their political-administrative sensitivity.

Based on our research, we advocate a stronger risk-based approach and future-oriented approach to risk management, however without replacing the existing instruments, methods or reporting methods as these are valuable as well. The risk-based approach is defined here as “the application of the six generic risk process steps in work processes” (Van Staveren, 2015, p. 79). The six generic process steps he identifies are: (1) determine the objectives, (2) identify the risks, (3) classify the risks, (4) manage the risks, (5) evaluate the risk management measures, (6) reporting. It is, however, different from traditional risk management in other ways as well. In a risk-based approach the focus is on achievement of the objectives, rather than implementation of a method. It is, much

more than in a conventional risk management approach, left to the discretion of teams, program managers and management themselves how they seek to achieve the risk management objectives at the level of projects, programs and strategy. For example, the previously mentioned risk diagnosing methodology, the precautionary principle, and the risk governance approach, are all instruments/principles/approaches that could be used to achieve particular risk management objectives.

A risk-based approach is different from the traditional risk management approach, in the sense that it assumes variation and expects people to be able and willing to make (business or policy related) choices. It invites and promotes cooperation and change instead of enforcing this, and seeks to design and develop in consultation and dialogue, instead of prescribing, regulating or enforcing what (not) to do. A risk-based approach is an approach where ownership is put at the level where it matters: policy makers, portfolio holders, team leaders, program directors, members of the management team, Director-General or Secretary-General.

---

#### WHICH INSIGHTS FOLLOW FROM THE SCIENTIFIC DEBATE?

The internal notes and policy documents of DGPol provide a number of directions for further design of risk management within the organization: (a) risk management should not only be geared to Plan and Control (P&C), but also towards 'Sense and Respond', (b) it should take into account the public and political accountability challenges within the complex political-administrative context of DGPol, and (c) informal stakeholder management should be part of risk management at DGPol. Are these suggestions valid, when we compare this with the scientific knowledge in these areas? An analysis of the scientific literature provides us with the following conclusions:

1. Sense and Respond is not appropriate as underlying (scientific) approach for DGPol, since DGPol is an organization with public and political accountability. Furthermore, the implementing organization has a hierarchical structure that does not match the 'sense and respond' approach as described in scientific literature.
2. Sense and Respond does, however, provide new insights and valuable points of departure for a risk-based approach, in particular in relation to weak signal recognition and in dealing with future uncertainties using foresight planning. Foresight planning is the process of scenario development, visioning, and planning and can be applied very well in combination with strategic stakeholder management.
3. Weak signal recognition should not only be used for risks in relation to projects or transition processes, but also to recognize *moral hazard* and *adverse selection*<sup>5</sup> when and where it occurs. In that case, partners have an alternative agenda, or they withhold information, which can result in major political-administrative risks.
4. Weak signal recognition does not just happen by chance. Weak signal recognition can be strengthened by the use of (a) environmental scanning, (b) issue management, (c) early warning at strategic level and (d) pattern recognition (Kuosa, 2010, see figure SC2).
5. Risk management and stakeholder management can mutually reinforce one another. One can distinguish between general stakeholder management and stakeholder management organized around themes or issues. Both are valuable. Issue-based stakeholder management can have great added value in relation to particular themes or within a particular area such as ICT (Roloff, 2007).
6. One needs to distinguish between strategic and moral stakeholders. A strategic stakeholder is a stakeholder who can contribute to, or hamper, the achievement of objectives in the organization; a moral stakeholder is the one who is affected by the (non)achievement of the organization's objectives (Frooman, 1999). The moral stakeholder is often depicted as a victim in mediatized incidents. It is recommended to take the perspective of moral stakeholders into account.

---

<sup>5</sup> The concepts 'moral hazard', 'adverse selection', and 'foresight planning' are further elaborated in chapter 3.



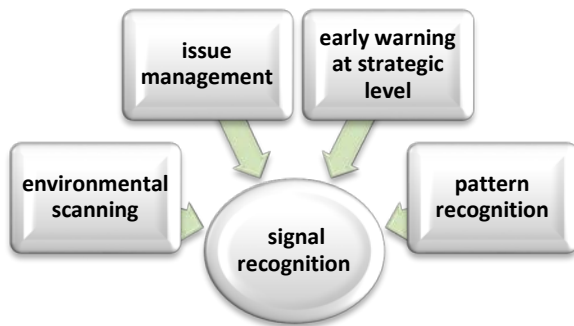


Figure SC2: Processes that facilitate weak signal recognition. (Based on Kuosa, 2010)

## STANDARDS AND FRAMEWORKS

With this in mind, and with our understanding of the risk concept, risk management, the risk governance approach and the risk-based approach, one can assess how suitable the available (conventional) risk management standards/frameworks are for application by DGPOL. The list of ‘selection and design criteria’ in table SC3 incorporates the necessary criteria as expressed by the respondents as well as insights from scientific literature (chapter 4). Using the information from the second national research project on risk management in the Netherlands (NBA, Nyenrode, Rijksuniversiteit Groningen, PWC, 2014<sup>6</sup>) and literature research on standards in use, we have assessed the following risk management standards and/or frameworks: COSO-ERM (2004), INK/EFQM, ISO 31000 (2009), Lean6Sigma, Basel II, Solvency II, Management\_of\_Risk, AS/NZS 4360 (2004), OCEG, AIRMIC, PRINCE 2®: COBIT, RISMAN and the Risk Diagnosing Methodology (RDM).

Table SC1: Selection and design criteria

selection criteria	ontwerpcriteria
<ul style="list-style-type: none"> <li>• generic</li> <li>• common in the Netherlands</li> <li>• transcending the project-level</li> <li>• user friendly</li> <li>• result oriented</li> <li>• flexible</li> </ul>	<ul style="list-style-type: none"> <li>• dialogue between policy and implementation</li> <li>• public accountability</li> <li>• has advantages for users</li> <li>• aligns with work routines and processes</li> <li>• promotes relation with stakeholders/partners</li> <li>• encourages situational awareness</li> <li>• encourages thinking out of the box</li> <li>• allows for sensitivity and plan &amp; control</li> <li>• is applicable in the political-administrative context</li> </ul>

The assessment resulted in ISO 31000 (2009) as most suitable framework for risk management at DGPOL. The principles and guidelines of ISO 31000 provide a framework for risk management that can be used by any organization, regardless of size, activity or sector. The ISO principles and technical guidelines allow for flexibility in the follow-up by the organization itself. This is no luxury, given the requirement for alignment with the tasks and characteristics of the organization itself. One of these features is that DGPOL is undergoing transformation itself. The

<sup>6</sup> This study provides information on the risk management frameworks/standards in use among 727 companies/organizations in the Netherlands with a budget or turnover over 10 Million Euro. See also: Paape and Speklé (2012).

amount of tasks is being reduced and also the focus of DGPoI is shifting. Providing direction, connection and management are gaining relevance compared to implementation and support. During recent years, significant changes have taken place, creating tensions and pressures on the relation between stakeholders and partners. The context within which DGPoI operates is also subject to change. Uncertainties in relation to the achievement of objectives have increased substantially, because many transitions and changes are taking place simultaneously, contributing to adverse spillover effects. Moreover, security and the police organization are always under scrutiny of parliament and media. Critical questions by the media are the order of the day. This means that DGPoI should have a great sensitivity for the political-administrative context and urgency.

A conventional risk management approach does not fit with that reality. We therefore recommend a combination of ISO 31000, a risk-driven and future-oriented approach to risk management, with emphasis on the political-administrative context. The combination is well-suited, since the six steps in the risk-based approach (according Van Staveren, 2015, p. 79) and the risk process of ISO 31000 (2009) are very similar (see figure SC3). The chapters in the figure refer to chapters in ISO 31000.

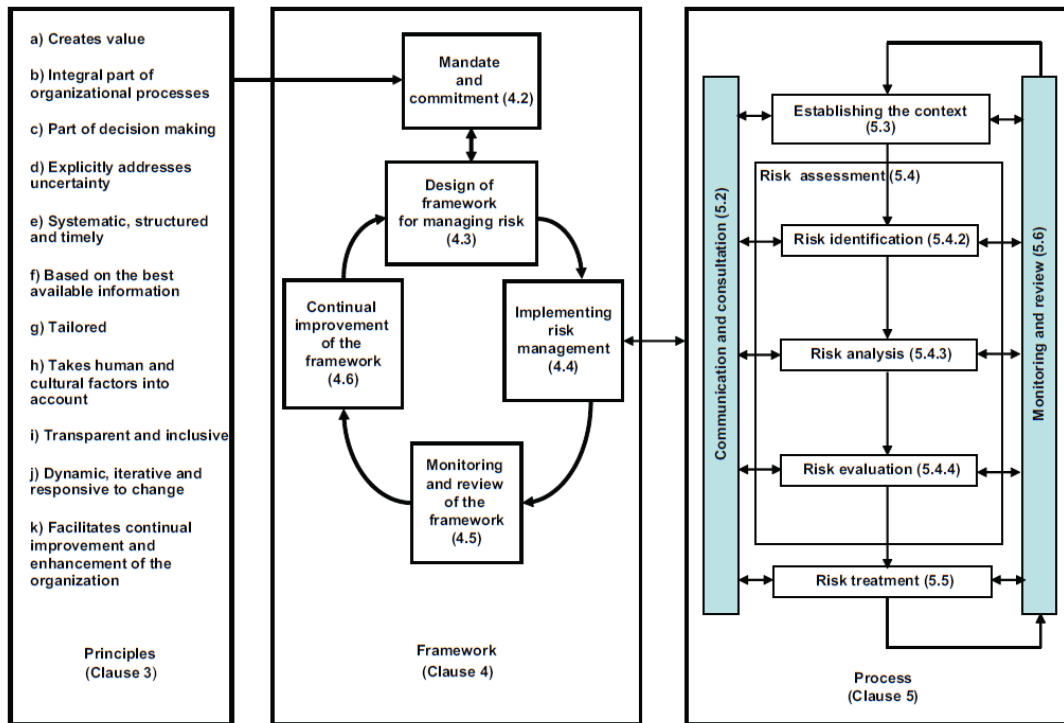


Figure SC3: ISO 31000: Principles and guidelines. Source: ISO 31000 (2009, p. vii).

## RISK MANAGEMENT – IN PRACTICE

Several staff members of DGPoI actively encouraged the introduction of a risk-oriented approach to risk management in the organization, and drafted several policy papers to this effect. In these papers, the initiators explored the concepts, underlying assumptions, the process and defined further steps for implementation of risk management in the organization. The risk process is at present most visible in the P&C cycle, in the budget cycle and in project management. The P&C cycle includes a planning/calendar with notes when which products should be delivered. The quarterly reports play a role in ensuring accountability. The P&C cycle includes an annual planning for next year; progress of implementation of the current year; and accountability over previous year.

Decision making on risks takes place at three levels of control in the organization: the concern controller of financial and economic affairs (FEZ), the controller of the DGPol, and the controller at program level. Risk assessments and analyses are implemented as integral part of the P&C cycle, with reporting taking place at the level of the department, in quarterly reports and in annual plans. The dashboard system is the most common method applied, and also used to start the dialogue on risks, progress, adjustments and risk management measures, between the financial department and control, and the other 8 policy programs; between DGPol and the National Police, between the Director-General (DG) and the Secretary-General (SG). The pSG cluster conducts risk assessments to enhance strategic decision making, or after major incidents.

When looking at the ISO principles one by one, one can conclude that all principles are addressed by DGPol in one way or another. For example, the risk management is incorporated in some P&C processes and is part of the decision making process at several points in time. Risk assessments are a part of the P&C cycle and reporting is done in the quarterly reports and annual plans. However, the execution of this is rather haphazard and the perceptions on the effectiveness of these measures are mixed. It is not sufficient to refer to this as ‘systemic, structured and timely’ risk management. The ‘maturity’ of risk management at DGPol is thus quite limited.

These findings cumulate in a number of conclusions for a risk-based approach at DGPol. First of all, it is important to invest time and dialogue in further translation of the ISO-principles in combination with a risk-based approach, tailored to the political-administrative context within which DGPol operates. A governance structure is required that facilitates and encourages risk-based approach, instead of a structure that prescribes each component in great detail. Most headway can be made in the systematic application of the risk process in strategic decision making, by explicitly defining risks in the political-administrative context, and by applying not only a risk-based approach but also a future-oriented approach to risk management.

---

## RISK MANAGEMENT – TOWARDS A DESIGN

Based on the research underlying this report, we suggest a risk-driven and future-oriented approach to risk management at program and strategic level, while maintaining the current and more conventional risk management instruments in the P&C cycle for the progress of projects and processes. In other words, we introduce different ‘colors’ in risk management, depending on the level, see figure SC4.



Figure SC4: Conventional risk management and a risk-based approach

A risk-based approach can, at all levels, be combined with the principles of ISO 31000, and tailored to the political-administrative context within which DGPol operates<sup>7</sup>. The risk-based approach thereby changes into a ‘principle-

<sup>7</sup> Table SC2 is supplemented with instruments and references in chapter 6.

based' and 'tailored' approach, as recommended by (ISO) principle 2.7.1: "Risk management is tailored. Risk management is aligned with the organization's external and internal context and risk profile." (ISO 31000, 2009, p. 8). In addition, we recommend application of future-oriented approach to risk management by means of foresight planning and scenario development. Mission, vision and strategy are key-elements of such an approach. Foresight planning consists of six steps: framing, scanning, forecasting (including scenario development), visioning, planning and acting (see table 3.1 from chapter 3). This can be further translated to (risk management) policy and objectives. Scenario development, which is one element in foresight planning, facilitates the mapping of strategic risks and uncertainties, to relate risk management to strategic decision-making and to make future choices more transparent.

Strategic management and a risk-based approach are closely interlinked, similar to risk driven approach to risk management and stakeholder management. Stakeholder management and strategic management are therefore included in figure SC5. It is to be expected that the principles from table SC2 and foresight planning mutually support and reinforce one another. While the principles can be used to support the process of foresight planning, similarly, the outcome of foresight planning may well contribute to further adjustment of the principles.

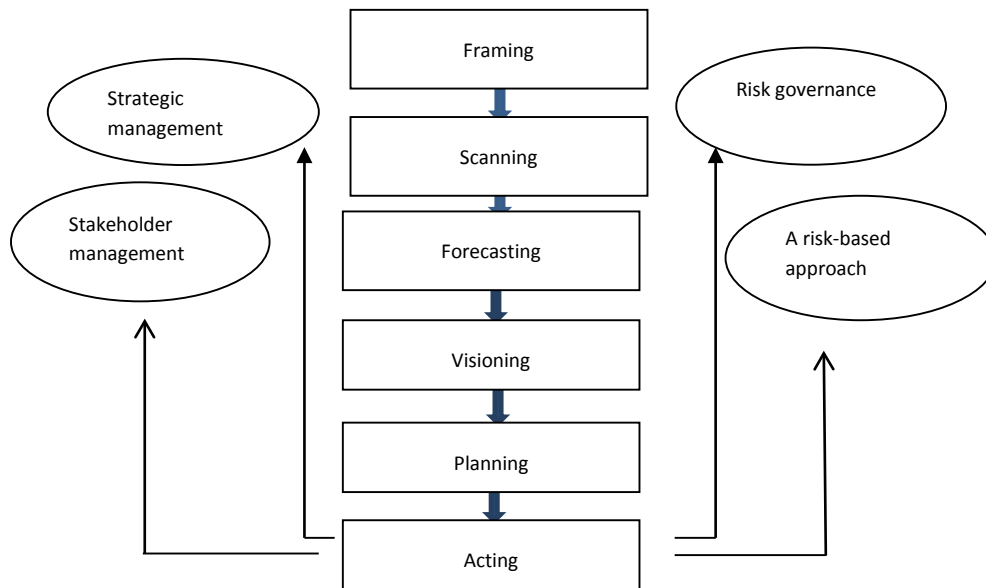


Figure SC5: Foresight planning (including scenario development) and feedback to risk management

Nr.	ISO Principle	A risk-based approach with a political-administrative focus:
2.1.1	Risk management creates and protects value.	<p>Creates value and contributes to the demonstrable achievement of objectives by:</p> <ul style="list-style-type: none"> <li>• recognizing and reducing political-administrative risks,</li> <li>• an effective response to questions by journalists; politicians; and to social unrest,</li> <li>• improvement of the accountability vis-à-vis regulators or supervisory authorities.</li> </ul>
2.2.1	Risk management is an integral part of all organizational processes	<ul style="list-style-type: none"> <li>• invites participation in consultation and dialogue,</li> <li>• is integral part of staff members' awareness,</li> <li>• is integral part in the cooperation with stakeholders and partners,</li> <li>• is integral part in the knowledge agenda of DGPol.</li> </ul>
2.3.1	Risk management is part of decision making	<ul style="list-style-type: none"> <li>• applies the risk process to political-administrative risks at strategic level,</li> <li>• creates ownership among staff at all levels for recognition of political-administrative risks, based on weak or strong signals,</li> <li>• makes political-administrative risks a subject of discussion in meetings of MT POL, MT POL Plus, PHO and team consultations.</li> </ul>
2.4.1	Risk management explicitly addresses uncertainty	<ul style="list-style-type: none"> <li>• refers explicitly to political-administrative complexity, uncertainty and ambiguity (including controversies) and adjusts the organization's strategy accordingly.</li> </ul>
2.5.1	Risk management is systematic, structured and timely	<ul style="list-style-type: none"> <li>• is dynamic, cyclic, interactive and asks questions in time,</li> <li>• uses accountability processes to learn and to secure improvements,</li> <li>• provides advice on risks well in time, and identifies the need for strategic change.</li> </ul>
2.6.1	Risk management is based on the best available information	<ul style="list-style-type: none"> <li>• is based on the best available information within the organization, in such a way that weak signal recognition is enhanced; that questions can be answered effectively; and learning is encouraged,</li> <li>• is based on the best available information from partners and/or stakeholders,</li> <li>• creates mutual interest among partners/stakeholders to share information.</li> </ul>
2.7.1	Risk management is tailored	<ul style="list-style-type: none"> <li>• takes explicit account of risks in the political-administrative playing field,</li> <li>• takes explicit account of the political, economic, the judicial and professional rationality in recommendations to the Minister,</li> <li>• takes explicit account of risks that follow from political-administrative changes,</li> <li>• takes explicit account of the complexities, uncertainties and ambiguities that are inherent to the process of cooperation with others.</li> </ul>
2.8.1	Risk management takes human and cultural factors into account	<ul style="list-style-type: none"> <li>• is aware of political-emotional argumentation or political pressure,</li> <li>• takes explicit account of relations between top level management and the minister,</li> <li>• takes explicit account of psychological factors (prestige; group think, desire to get something accepted).</li> </ul>
2.9.1	Risk management is transparent and inclusive	<ul style="list-style-type: none"> <li>• creates awareness of political-administrative risks among staff at all levels,</li> <li>• encourages staff to better recognize weak signals,</li> <li>• makes political-administrative risks a subject of discussion in meetings of MT POL, MT POL Plus, PHO and team consultations.</li> </ul>
2.10.1	Risk management is dynamic, iterative and responsive to change	<ul style="list-style-type: none"> <li>• is dynamic, iterative and responds to societal changes,</li> <li>• is future-oriented and looks beyond the legislative term.</li> </ul>
2.11.1	Risk management facilitates continual improvement of the organization	<ul style="list-style-type: none"> <li>• encourages continuous development and improvement of the risk-based approach,</li> <li>• analyzes data upon questions from media, parliament, supervisory authorities, and makes adjustments to policy based on the lessons learned.</li> </ul>

## FINAL CONCLUSION AND RECOMMENDATIONS

This research addressed two main questions. The first question was:

A. What is the standard or framework (or combination thereof) for risk management, that can be applied by DGPoI and fits best with the specific tasks and characteristics of DGPoI, the specific needs with regard to risk management, in particular the relation with the political-administrative context of DGPoI?

The choice for the ‘best’ standard, framework or approach, is closely related to the risk management objectives of the organization. If DGPoI wants to show that it is ‘in control’ with regard to its projects, programs, transition processes and strategies, then it is evident that further development, adjustment, and implementation of conventional risk management methods is required at a much higher level of risk maturity. If DGPoI wants to look forward, and if it wants to make clear choices, then a risk-based approach is more suitable and in line with the ambitions as formulated in the Ambition Document. While some methods from the conventional approach are useful, we found that a pure conventional risk management system does not fit with the political-administrative context in which DGPoI operates. In this research we argue in favor of a combination of ISO 31000 and a risk-based and future-oriented approach. The second question follows from the first:

B. How can the selected standard or framework be embedded in the structure, work processes and reporting of DGPoI in such a way that it is aligned with the specific tasks and characteristics of DGPoI and the specific needs with regard to risk management, in particular in relation to the political-administrative context of DGPoI?

*Conclusion 1:* A risk-based and future-oriented approach should take account of the tasks, characteristics, needs and the political-administrative context of DGPoI, as is also done in this research. In answering the questions, we discussed not only standards and frameworks for risk management, but explored several issues that are directly related to public administration and public management. This creates more opportunities for an organization-wide integration of a risk-based approach, and should therefore get priority in further enhancement of risk management.



Figure SC6. Domains of a risk-based approach within DGPoI

Risk management thereby shifts from a 'mono-discipline' and 'issue management' to an organization-wide strategy that also offers advantages in other areas as well. This will not be realized within one day, but is a task that can be further explored and demarcated by staff members, directors and managers, according to the principles of a risk-based approach and ISO 31000 (2009).

*Recommendation 1:* Request the risk manager of DGPol to draft a planning for further operationalization of each of the domains in figure SC6. Include targets in this planning. Several prospects for action and various literature sources can be found in this report for further reference. This enables DGPol to gradually gain more and more control over the risks in the programs executed by her.

*Conclusion 2:* Risks are often defined as 'probability times effect' or variations thereof. An extensive literature research reveals that this definition is strongly criticized, for several reasons. The most important conclusion is that this commonly-used definition is not applicable to risks "that are characterized by high levels of complexity; uncertainty and ambiguity" (Renn, Klinke and Van Asselt, 2011, p. 234). Many of the risks that DGPol has to deal with at a program and strategic level, have such characteristics.

*Recommendation 2:* examine the individual program annual plans within DGPol with regard to complexity, uncertainty and ambiguity. Apply the 'Risk Diagnosing Methodology' (section 4.3.14) in case of innovation and complex transition processes; apply the precautionary principle (box 2.1) in case of major uncertainties; and apply the organization-transcending 'risk governance' approach (fig. 2.1) in combination with stakeholder management in case of complex administrative decision-making with multiple stakeholders or partners.

*Conclusion 3:* a pure conventional risk management approach does not fit with the political-administrative context within which DGPol operates. In this research, we argue in favor of a combination of ISO 31000 with a risk-based and future-oriented approach. The overall goal of a risk based approach is the achievement of objectives, not the introduction and enforcement of a method.

*Recommendation 3:* Jointly discuss the risk management objectives. Check the ambition document 'D1000' with the ISO principles, using the checklist from table SC2, and formulate a plan of action to realize those characteristics and goals from the ambition document that have not yet been realized. This will increase the collective risk awareness within DGPol. involve, where possible, stakeholders and partners in the discussion.

*Conclusion 4:* Further exploration and implementation of weak-signal recognition is required given the potential risks and accountability processes in the political-administrative context.

*Recommendation 4:* Appoint someone in the organization to further explore the actions required for weak signal recognition. Facilitate weak signal recognition using the suggestions from chapter 3. Convert weak signals of potential high political-administrative risks into strong signals, by asking supervisory authorities to look at it. This increases the trust of regulators and supervisory authorities in DGPol's commitment to careful consideration of risks and risk response mechanisms.

*Conclusion 5:* more awareness of future challenges, can result in another view on the future direction and capacities of the organization. A basket of methods and techniques is available to explore the scenarios and future options, and is referred to as 'scenario development' and 'foresight planning'.

*Recommendation 5:* Apply a gradual introduction of foresight planning and scenario development at DGPol (see p. 76 and on), e.g. by introduction in phases per DGPol program. In this way, it is possible to relate risk management to strategic decisions, and to create more transparency about future choices for each program.

*Conclusion 6:* The risk-based approach benefits from increasing knowledge in the organization about risks, risk response mechanisms or measures, and approaches that fit with the type of risks that DGPol is facing.

*Recommendation 6:* Apply the three measures in box 6.1 to integrate knowledge in the current (heuristic) risk management. This increase awareness, commitment and competencies of staff members in the organization to further enhance and implement a risk-based and future-oriented approach.

*Conclusion 7:* A major advantage can be reached by applying the risk (analytical) process (ISO 31000) to strategic decision-making and by making risks in the political-administrative context explicit.

*Recommendation 7:* carry out a pilot with the introduction of the 'questionnaire political-administrative risks' (section 6.5.1) in the regular policy cycle. If successful, the introduction can be considered for DGPol - wide.