DISCLAIMER

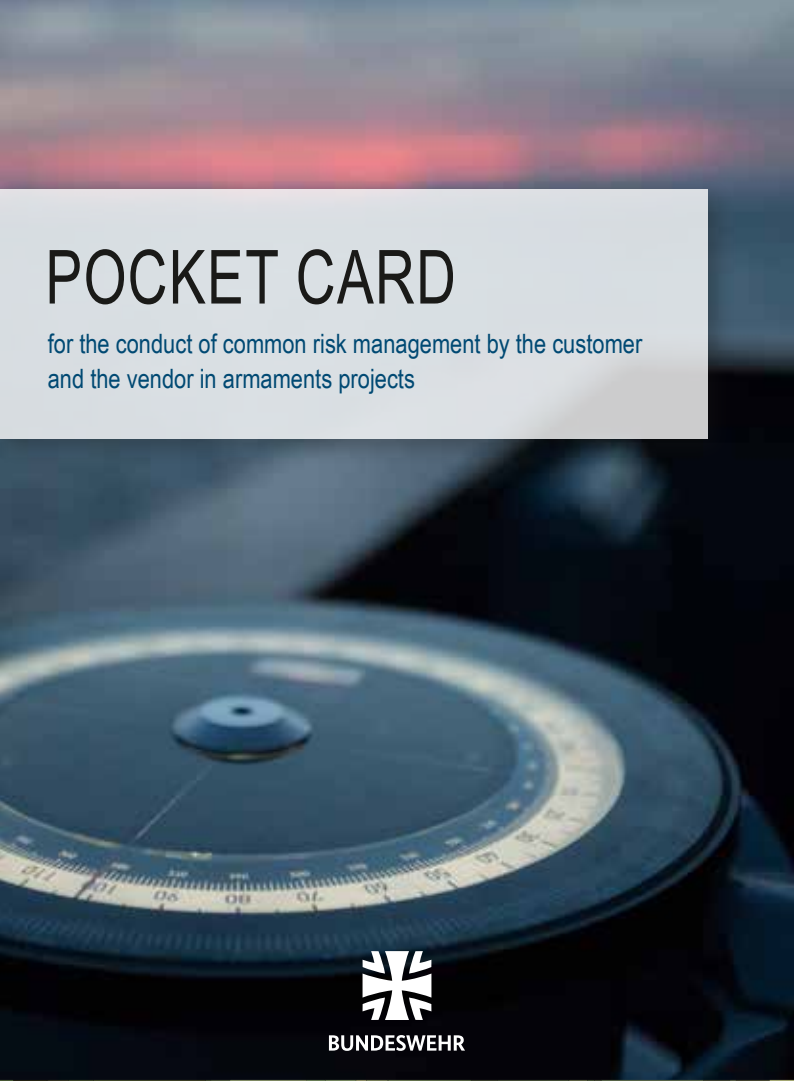
Information on the "Common Risk Management" pocket card used within the BAAINBw and by the vendors

- The pocket card "Common Risk Management" developed in collaboration with the BDSV is intended to foster a common basic understanding of risk management and serves as a starting point for conducting common risk management meetings.
- In projects without explicit contractual provisions on risk management (which have been the rule up to this point), it serves as a non-binding resource for vendors offering suggestions on the most important contents and methods of risk management.
- It is a compromise between the method used by the vendors and the applicable regulations for the customer's armaments management.
- For the customer (BAAINBw), the provisions for risk management in the performance process "Providing material solutions iaw CPM" remain binding according to Joint Service Regulation ZvD A1500/30 "Risk Management in Armaments Management".
- This pocket card does not replace the internal Bundeswehr administrative regulation.
- Differences in content between the pocket card and ZvD A1500/30 consist primarily in the risk evaluation (risk matrix) as well as the thresholds for the categories of likelihood of occurrence and magnitude of damage.

BUNDESWEHR

POCKET CARD

for the conduct of common risk management by the customer and the vendor in armaments projects



BUNDESWEHR

COMMON RISK MANAGEMENT BY CUSTOMER AND VENDOR

- For armament projects, there is a special focus on the budget and the constraints of budgetary law, which is usually combined with a tight schedule.
- The cost and financial management of these projects is frequently based on an approach which does not consider any budgets for preventing and handling risks.
- In conditions like these, a close and professional cooperation between the contractor and customer is crucial for the success of complex (large) projects.
- Common risk management helps to ensure project success by jointly managing and organising project risks.
- Common risk management should be understood as a value-added part of the report, project, and knowledge management and be integrated into the projects.
- Risk management within the project must be seen as a shared task:
  - Competencies on the customer and the vendor side are integrated
  - Creation of a common, transparent situation picture
  - Definition of common countermeasures to achieve the project objectives
  - Possible consequences have a high degree of transparency and can be evaluated jointly.

BDSV

BUNDESWEHR

PRINCIPLES OF COMMON RISK MANAGEMENT

Risk management is a shared task

Routines are drawn up for early identification of risks

Opportunities and risks are communicated pro-actively

The assessment of risks is done according to similar systematics (without binding guidelines iaw the included assessment matrix)

Measures are defined for each risk

Measures are continuously monitored

The status of measures is known to the partners

Common reviews support risk management

Consideration given to all three project dimensions: Time/deadlines, costs/funding, and performance/quality

COMMON RISK MANAGEMENT PROCESSES

1. **Identify risks**
   - Brainstorming
   - FMEA
   - Risk workshops
2. **Analyse risks**
   - Risk description
   - Analysis of effects
   - Analysis of causes
3. **Assess risks**
   - Probability of occurrence
   - Level of damage (scheduling delay, costs)
   - Risk categories
4. **Determine measures**
   - Define measures
   - Evaluate effectiveness
   - Designate responsibility
5. **Track risks and measures**
   - Monitor measures
   - Verify effectiveness
   - Perform reviews

RISK IDENTIFICATION

Are new risks continuously identified?

Which methods are used for risk identification?

Are experts involved in the identification?

How are new risks communicated pro-actively?

Is there an exchange between the customer and the vendor (common risk meetings)?

Did an exchange with other projects occur (e.g. lessons learned)?

RISK ANALYSIS

Are the risks described?

Is an analysis of effects performed across all dimensions (time/deadlines, costs/funding, and performance/quality)?

Is a systematic analysis of causes performed (e.g. cause-effect-chart, fault tree analysis, FMEA)?

Is the analysis of causes carried out in interdisciplinary teams?

Are the results documented?

RISK ASSESSMENT

Probability of occurrence

Factor	Assessment	Description	Probability
5	very likely	Will almost always occur	90% - 99%
4	likely	Will occur in most cases	70% - 89%
3	possible	Will occur in some cases	30% - 69%
2	unlikely	Not expected to occur	10% - 29%
1	very unlikely	Will usually not occur	1% - 9%

Level of damage or scheduling delay

Factor	Max Assessment	Description	e.g. contract € 500,000,000	e.g. duration
6	critical	e.g. delayed delivery	e.g. > € 50,000,000 (>10%)	e.g. > 7 months (>10%)
4	high	e.g. high development risk	e.g. € 25,000,000 (5%)	e.g. 4 months (5%)
3	medium	e.g.		(2%)
2	low	e.g. warranty case	e.g. € 5,000,000 (1%)	e.g. 1 month (1%)
1	minor	e.g. price increase	e.g. < € 5,000,000 (<1%)	e.g. < 1 month (<1%)

to be defined for each specific project

RISK PRIORITY NUMBER

			Level of damage or scheduling delay				
			minor	low	medium	high	critical
			1	2	3	4	5
Probability of occurrence	very likely	5	5	10	15	20	25
	likely	4	4	8	12	16	20
	possible	3	3	6	9	12	15
	unlikely	2	2	4	6	8	10
	very unlikely	1	1	2	3	4	5

Risk class		RPN	Description
Category 1	very high	>16	Extremely high, unacceptable risk, immediate measures required, management on project sponsor or vendor's management level
Category 2	high	13-16	High risk, project manager's attention (customer, vendor)
Category 3	medium	7-12	Moderate risk, exercise leadership responsibility on intermediate levels
Category 4	low	1-6	Low risk, use routine procedures at employee level

COMMON POTENTIAL RISKS

- Changes to the requirement situation and uncertain requirements
- Unrealistic timetables and budgets
- Provisions and assistance not meeting time and cost requirements
- Insufficient availability of resources
- Demonstration of integrated equipment and systems
- Lack of supportability and logistics
- Interconnections and dependencies with other projects
- IT security requirements
- Unsuitable/civil/tightened rules, standards, and regulations
- Obsolescence
- Room for interpretation in the technical specifications
- Development activities in the project

(Selection and order do not claim to be exhaustive or prioritised)

EDITORIAL INFORMATION

Published by:
Federal Ministry of Defence
Stauffenbergstraße 18, 10785 Berlin

Contact us:
Federal Ministry of Defence
Staff element risk management in the Directorate-General for Equipment – A RC
Stauffenbergstraße 18, 10785 Berlin

E-Mail: bmvgarc@bmvg.bund.de

Cover picture: © Bundeswehr/Twardy

Layout/typesetting/print:
BAIUDBw Section DL I 4,
Zentraldruckerei BAIUDBw
Intranet: http://zentraldruckerei.iud

This publication was developed in cooperation with the Federation of German Security and Defence Industries (BDSV). It is distributed free of charge and is not intended for sale.

BUNDESWEHR