Risk Management Manual

Version as at: October 2018

Preface

The risk management system of an enterprise is intended to optimally handle already in advance the risks to which the enterprise may be exposed, thus minimizing the economic impacts.

An effective risk management system is not only an economic necessity, it is also required by law:

The German Act on Supervision and Transparency in Businesses (*Gesetz zur Kontrolle und Transparenz im Unternehmensbereich – KonTraG*) requires the management board to ensure that appropriate risk management is in place.

The German Act on the Modernisation of Accounting Law (*Bilanzmodernisierungs-gesetz – BilMoG*) specifies the supervisory board's duties of supervision. The supervisory board's responsibilities include monitoring the effectiveness of the internal control system (ICS), the risk management system (RMS) and the internal audit system.

Moreover, section 3.4 of the German Corporate Governance Code (http://www.dcgk.de/de/kodex.html) provides that "the management board shall inform the supervisory board regularly, promptly and comprehensively about all matters important to the enterprise with regard to strategy, planning, business development, risk situation, risk management and compliance".
Section 4.1.4 stipulates: "The management board shall ensure appropriate risk management and risk controlling".

This Risk Management Manual is divided into a general and a specific part and applies currently to all central business and organisational units of BayWa AG as well as to all of BayWa AG's subsidiaries/integrated affiliates.
For organisational reasons, RWA and the subsidiaries/affiliates attributed to it operate their own risk management system. The two risk management systems are harmonised as far as possible, ensuring an overview of the risks of the Group.

The general part of this Manual provides general information regarding risk management, its process and on how the risks are handled.

The specific part contains the organisational policies and definitions regarding the risk management system and the risks within the BayWa Group.

The risk management system and this Risk Management Manual are designed as work in progress to be adapted based on the experiences and suggestions made by their users.

Munich, October 2018

Table of contents

Introduction

The risk management within the BayWa Group is divided into the following two segments, which each carry out an individual risk management:

- BayWa AG including its subsidiaries/integrated affiliates
- RWA AG including its subsidiaries/integrated affiliates

This division is made for practical reasons and is intended to emphasise the operative responsibility and to optimally support the risk management process.
The applied systems and processes are similar, but may vary in detail.
This Manual describes the risk management within BayWa AG including its subsidiaries/integrated affiliates (any references to BayWa AG hereinafter include its subsidiaries/integrated affiliates).

Objective

This Manual is intended to describe BayWa AG Munich's risk management system.

This Manual gives the staff members clear instructions on how to carry out the risk management processes.

This internal perspective with respect to the Risk Management Manual enables each staff member to obtain an overview of the overall system and thus an understanding of the correlations. In addition, such documentation is required to ensure the implementation of risk management measures.

From an external perspective, this Risk Management Manual is an instrument of the management to demonstrate that it has complied with its obligations under section 91 para. 2 of the German Stock Corporation Act (*Aktiengesetz – AktG*) and thus also an important basis for the audit to be performed by an auditor pursuant to section 317 para. 4 of the German Commercial Code (*Handelsgesetzbuch – HGB*).

Scope of application

The risk management has been included in the responsibilities of the subsidiaries/ integrated affiliates, central divisions and organisational units and is to be carried out by them on a continuous basis.

A. General

1. Legal basis

The legal basis of risk management is set forth in the German Act on Supervision and Transparency in Businesses.

The provisions of the German Act on Supervision and Transparency in Businesses apply primarily to listed companies and increase the duties of management boards, supervisory boards and auditors.

The German Act on Supervision and Transparency in Businesses was published on 27 April 1998 in the Federal Law Gazette (*Bundesgesetzblatt*), pp. 786 et seqq., and entered into force on 1 May 1998.

It contains provisions resulting in direct amendments to the wording of various rules and regulations:

- German Stock Corporation Act (Aktiengesetz – AktG)
- German Commercial Code *(Handelsgesetzbuch – HGB)*
- German Limited Liability Companies Act (*GmbH-Gesetz – GmbHG*)
- German Cooperative Societies Act (*Genossenschaftsgesetz – GenG*)
- German Public Disclosure Act (*Publizitätsgesetz – PublG*), etc.

The relevant passages of the German Stock Corporation Act and the German Commercial Code in respect of risk management will be addressed below in detail; the complete wording of the German Act on Supervision and Transparency in Businesses including further important provisions on risk management is available as **Annex A 1**.

Article 1 of the German Act on Supervision and Transparency in Businesses provides for section 91 para. 2 of the German Stock Corporation Act to be reworded as follows:

> “The management board shall take suitable measures, in particular surveillance measures, to ensure that developments threatening the continued existence of the enterprise are identified early.”

According to the legislative explanation of the draft bill, this means that the management board is required to ensure that appropriate risk management and appropriate internal audit processes are carried out. The wording of section 91 of the German Stock Corporation Act is attached hereto as **Annex A 2**.

Pursuant to section 317, paras. 2 and 4 of the German Commercial Code, auditors are also required to include risk management in the scope of their audit and report.

Section 317, para. 2	"...it shall also be examined whether the risks of the future development have been accurately represented"
Section 317, para. 4	"... it shall also be determined in the scope of the examination whether the management board has appropriately taken the measures imposed on it pursuant to section 91 para. 2 of the German Stock Corporation Act and whether the internal control system which is to be installed there under is able to perform its tasks."

2. Risk management definitions

2.1 Risk

In everyday language, the term “risk” refers to the possibility that things may turn out differently than expected.

Such broad definition includes both possibilities: positive developments and the negative perspective of threats or unfavourable developments.

The <u>definition of risk in the narrower sense</u> refers traditionally to a threat of damage or loss, with risk always being seen as an unfavourable, dangerous or existence-threatening development.

2.2 Definition of risk pursuant to the German Act on Supervision and Transparency in Businesses

The German Act on Supervision and Transparency in Businesses refers to the risk definition in the narrower sense.

Risk is consequently to be understood as the threat that losses may occur in connection with business activities.

Such losses may be incurred in individual transactions, in a business segment or in the company or group as a whole.

2.3 Definition of risk in relation to enterprises

When the risk definitions set forth above are applied to enterprises, they refer to the threat that events or measures prevent the enterprise from achieving its goals or from successfully implementing its strategies.

2.4 Risk management

Risk management refers to all organisational policies and measures used to identify and handle the risks associated with entrepreneurial activity.

Originally, the term risk management was limited only to the analysis and the handling of generally insurable risks of damage or loss. Of late and not only due to the German Act on Supervision and Transparency in Businesses, risk management is understood to include, apart from the identification and control of tangible risks, also the handling of speculative business risks.

The figure below shows the elements of a risk management system.

Elements of the risk management system

Controlling	**Internal control system/risk management of subsidiary/affiliate, individual business unit or organisational unit**	**Internal audit**
<u>Tasks</u> Defining and standardising risk identification, risk assessment, risk documentation, risk management measures, risk communication Coordinating the schedules and tasks of all units involved in the risk management system Central contact for all units involved in the risk management process Summarised risk reporting to the managment board	<u>Tasks</u> Coordination, advice and communication within the subsidiary, business unit or organisation unit Defining the tasks and responsibilities Monitoring the processes, functions and adopted measures (early-warning system) to identify risks at an early stage and to create options for action based on the awareness of the risks Documenting the tasks and responsibilities	<u>Tasks</u> Reviewing the functioning of the risk management system (see section B, chapter 3) Auditing the functionality of controls and measures in terms of risk management and control

2.5 Internal control system (ICS) and its integration with the risk management system

As shown in the figure in no. 2.4. (Risk management) above, the internal control system is considered to form a part of the overall risk management.

It contains all mechanisms of internal control, which can be situated upstream, downstream or at the same stage.

Main tasks of the ICS are safeguarding and protecting the existing assets against losses of all kinds, obtaining precise, meaningful and prompt records, furthering operational efficiency by analysing the obtained records and supporting compliance with the defined corporate policy.

An effective ICS requires the clear definition and organisation of workflows. In addition to work instructions, this also includes an appropriate form sheet system.

Several workflow functions should not be performed by one person or one organisational unit. Separation of functions has to be ensured.

Auditing the functionality of the risk management process as well as the controls and measures to manage and monitor the risks is performed by the internal audit department on a regular basis.

3. *Risk management objectives*

The definition below reflects the objectives of risk management comprehensively and objectively.

> "... early identification of risks potentially threatening the company's results of operations, financial position and net assets in order to create options to take measures permitting long-term safeguarding of existing and creation of new potential for success, thus ensuring the continued existence of the enterprise."[1]

Definition	Explanation
early identification	The proactive focus of risks prevents in the event of emergency a surprise associated with hectic and excessive or wrong reactions. Continuously including the risks in day-to-day work allows for action instead of reaction and provides the option of actively shaping the development
of risks potentially threatening the company's results of operations, financial position and net assets	The concept of "results of operations, financial position and net assets" might seem to be a reference to the annual financial statements, i.e. the balance sheet and the profit and loss account. Such view, however, is to narrow. Risks to the results of operations, financial position and net assets are not always reflected by the figures as clearly and promptly, i.e. not always in time. Risks to the corporate image or competition risks might not be appreciable and noticeable until later periods. The risk, however, exists already today, and today it is that we have to start eliminating the risk and counteracting any potential adverse impacts.
in order to create options to take measures	Timely corrective action avoids the situation where the enterprise would have to react

[1] KPMG, Integrated Risk Management, July 1998

	from a position of vulnerability. It creates the option to act, i.e. to shape the developments.
permitting long-term safeguarding of existing and creation of new potential for success,	Long-term safeguarding means to extend the planning horizon beyond the next year and to think strategically: where do we want to be in five or ten years? Existing, i.e. current success has to be preserved and to be continued in future. This does not mean, however, to rest on past successes; it is rather required to discover and exploit new opportunities.
thus ensuring the continued existence of the enterprise	By taking such proactive action, the employees ultimately secure the future and the continued existence of the enterprise and thus their own jobs.

4. Risk management principles and organisation

Risk management principles are documented rules of conduct on how to handle risks in an enterprise; at the same time, they are a reference point for the risk management organisation.

Drafting and communicating risk management principles is the responsibility of the management.

Such rules of conduct are intended to initiate and continuously enhance a sustainable process of establishing risk awareness and developing a risk and control culture.

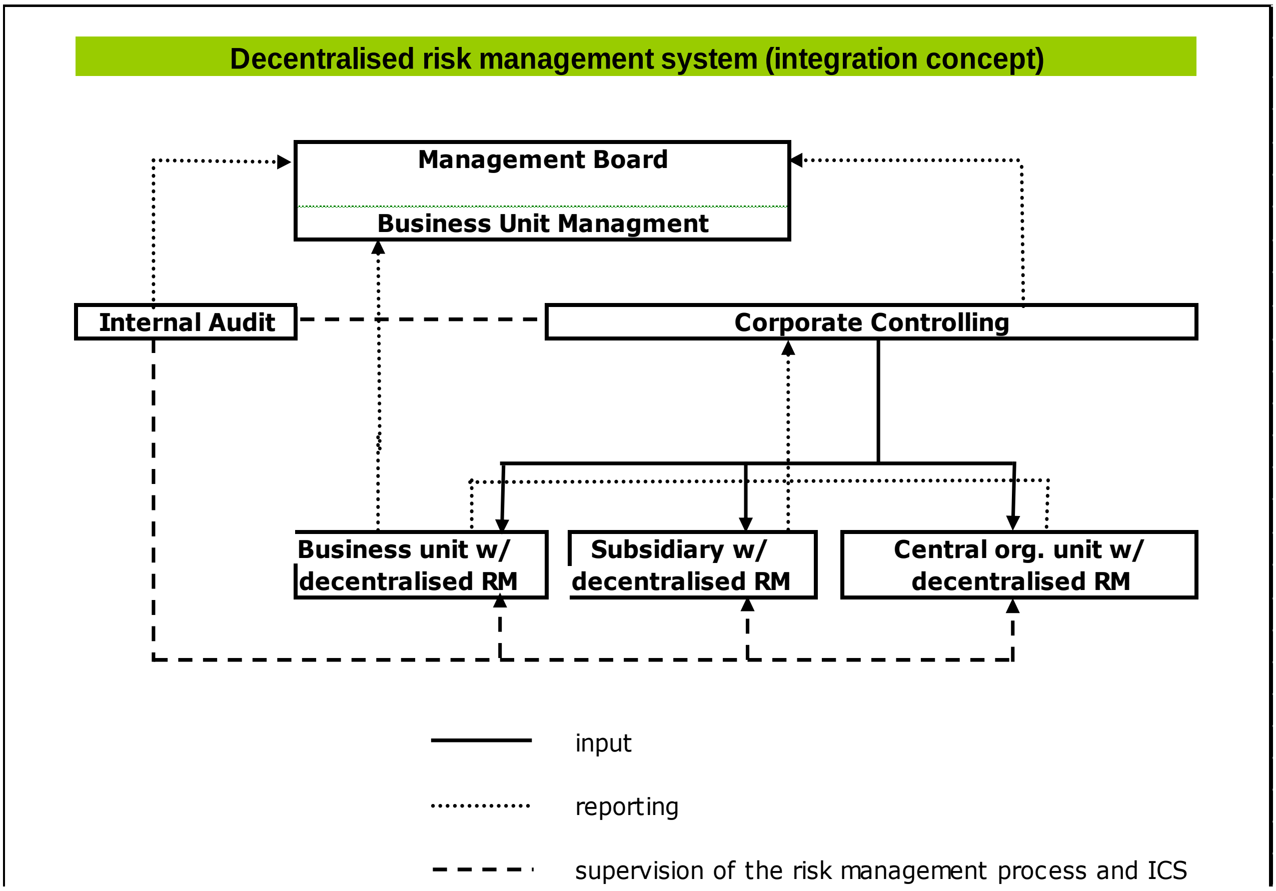
These rules are to be communicated top - down and complied with by all staff members.

The operative management has to set an example in following the guidelines and thus complying with the risk management principles. Risk management has to be embedded in the organisational and operational structures.

A central contact point supports the individual units in risk management matters.

The internal audit department is among others responsible for monitoring the effectiveness, appropriateness and efficiency and for identifying weak points.

Risk management organisation

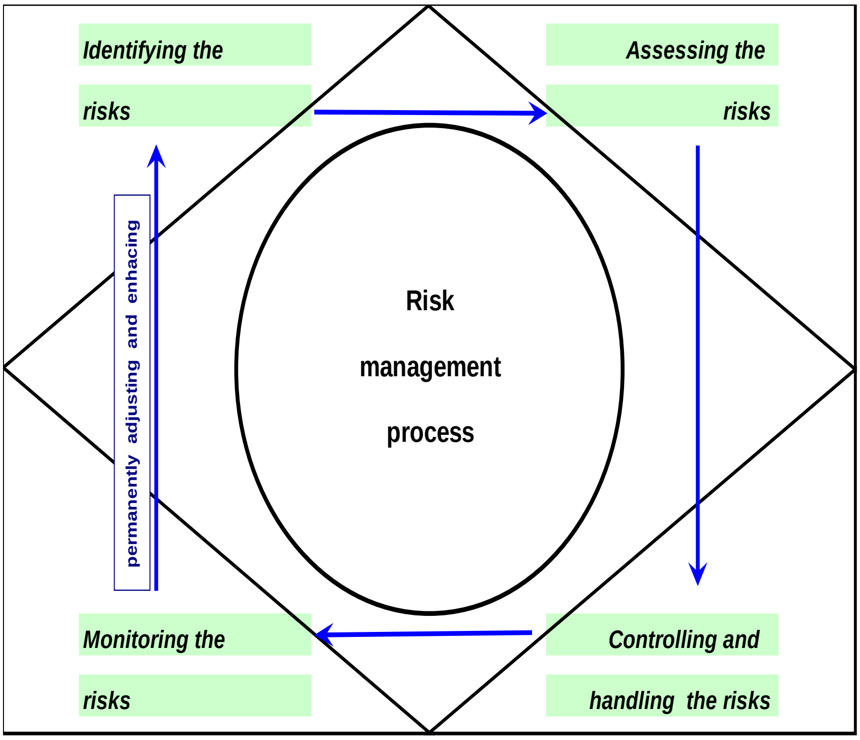


5. Risk management process

Risk management includes all activities intended to systematically deal with risks in business and is to be installed as a permanent task. Risk management is not an isolated process carried out in parallel to the actual business activities, but it is to be embedded in the existing business activities.

Risk management with its anticipatory view as to potential threats and their impacts on business success is to be incorporated as an integral part into strategy, medium-term planning and operative planning.

The approach for developing the risk management is illustrated in the figure below.



As a consequence, the risk management process consists of the following tasks:

- risk identification
- risk analysis
- risk communication
- risk control and documentation
- risk monitoring

5.1 Risk identification

At this stage, the material risks are identified.

At the risk identification stage, however, it is not clear yet whether the individual risk is a significant or a negligible risk, which is why all risks are to be recorded during the risk identification process (similar to a brainstorming process).

Although the German Act on Supervision and Transparency in Businesses refers to risks threatening the continued existence of the enterprise, the focus at the risk identification stage is on identifying all potential risks. Any monetary assessment or assessment of probabilities of the risks is not intended at this stage.

The identification of the risks is not a one-time task, but an ongoing process. Newly identified risks and detected changes in the situation of the individual risk are to be promptly recorded in the risk management system.
The risk identification process (risk inventory) is to be carried out according to functions or business processes.

5.2 Risk analysis

The objective of risk analysis is to further examine and evaluate the identified risks.

At this stage, risks are evaluated qualitatively and/or measured quantitatively; the basic information obtained is at the same time the basis for the next steps of the risk management process to be taken.

The evaluation or measurement of the risks has to relate to the original risk situation, i.e. the risk is to be assessed net of any effects of measures reducing or neutralising the risk.

The indicated amount of the value at risk and also the time by which the risk might materialise are estimates made based on certain assumptions, which reflect the actual event of occurrence only to a limited extent.

This fact has to be always borne in mind when further handling risks in the risk management system: there has to be a reasonable balance between costs and benefits.

The degree of the risk is determined by its probability of occurrence and the associated damage or loss.

Such basic information triggers at the same time the next steps of the risk management process to be taken, i.e. significant risks are recorded in the risk map and risks exceeding the threshold triggering a report to the management board are communicated to the management of the relevant division or the head of the relevant organisational unit, and to the overall management board.

5.3 Risk communication

A prerequisite for effective risk control is that the relevant decision-maker is promptly and appropriately informed by means of a suitable reporting system.

The framework for individual risk control measures is specified by guidelines to be defined by the management.

The degree of the risk defines the measures to be taken by the risk contact or the risk owner.

Significant risks and existence-threatening risks recorded in the risk map are to be permanently monitored. Expected risk occurences implying significant consequences, have to be communicated immediately and verifiably via the information chain to the relevant risk owner, the division's management and the central risk management (Mr Oberstadler).

5.4 Risk control and documentation

Risk control means directly exerting influence on the risks, i.e. this stage is about actively influencing them.

Depending on the strategic objectives of the enterprise, the risks assessed by way of the risk analysis in terms of probability of occurrence and amount of damage or loss are now to be

- reduced
- prevented or
- transferred

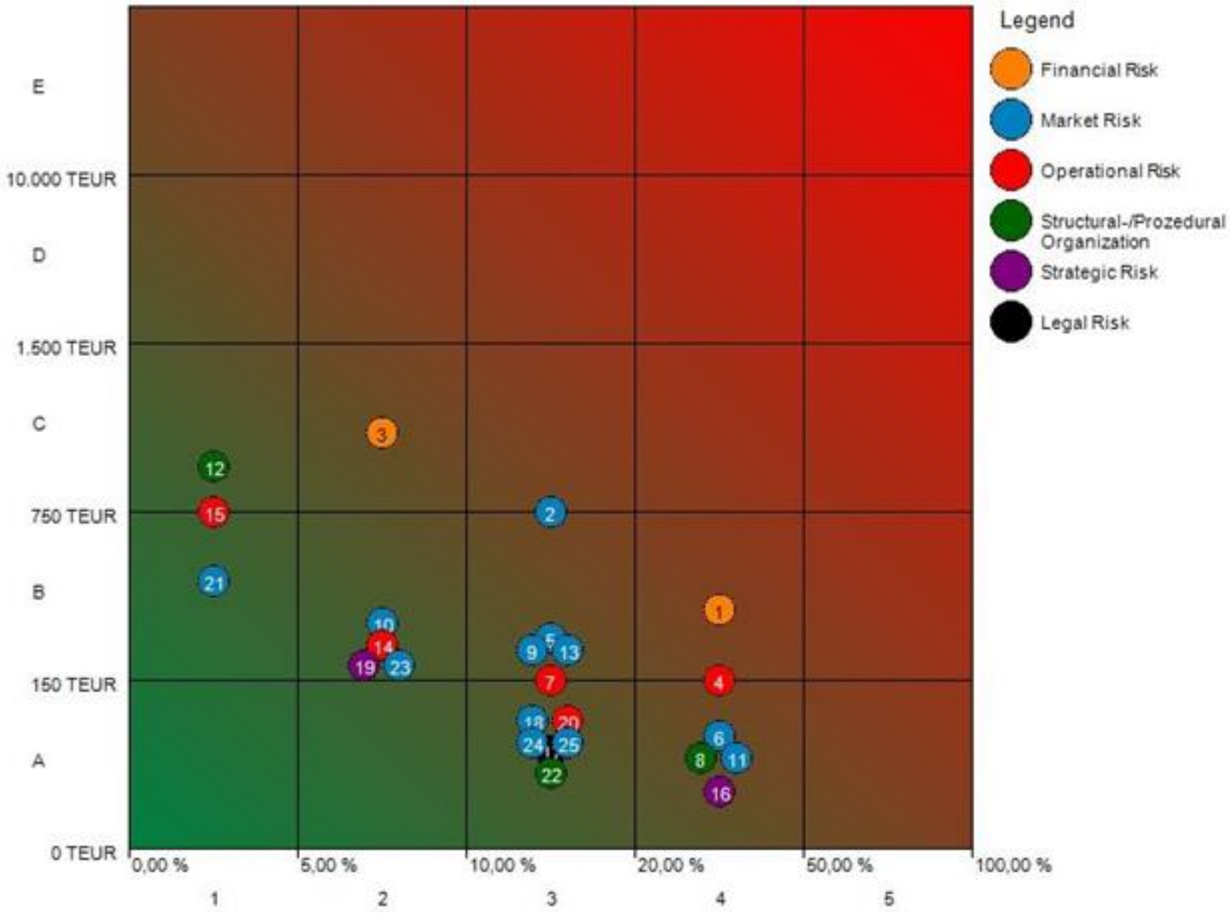
by taking control measures.

The approach for handling risks is generally contained in the risk management principles. In addition, the risk handling approach can be derived from the risk management objectives.

As a consequence of such operational understanding of risk, an identified and evaluated risk may also be accepted without taking any measures against it.

The handling will be depend decisively on where the individual risk is mapped in the below matrix.

Risk matrix



The risks, amounts of damage or loss, measures and control mechanisms are recorded in a risk map in order to ensure awareness of significant risks, to monitor risks and ultimately also to provide proof that risk management is being carried out as required by the German Act on Supervision and Transparency in Businesses. The recordings are to be made at periodic intervals.

The measures and control mechanisms used to control the risks are of particular importance in risk documentation. The implementation of such measures is to be monitored on an ongoing basis. This is the only way to ensure effective risk control.

5.5 Risk monitoring

The last step of the risk management process consists of monitoring the risks by comparing target and actual data. In doing so, the measures and their desired effects are monitored.

It is continuously monitored whether the risk control measures serve their intended purposes.

The monitoring is carried out by the staff members integrated in the process.

Identified deviations are to be analysed and documented in the risk management system. In addition to the data evaluation, the decisive steps are communication and, where required, corrective action.

6. *Risk management supervision*

In relation to the individual risk and how to handle it, the risk management system described above is supervised by the affected staff members themselves by way of the monitoring process integrated in the workflow.

The entirety of the risks, however, needs to be supervised externally, although externally does not necessarily mean by third parties.

Such external supervision is indispensable to detect flaws existing in the risk management system, in particular in the risk management organisation and in the risk management process (interface problems).

Such supervision of the risk management system is typically carried out by the internal audit department, but may also be delegated to external experts.

B. Risk management in BayWa AG
(including subsidiaries/ integrated affiliates)

1. Risk management principles of BayWa AG

These principles have been set forth by the management; they are included in the corporate guidelines.

The corporate guidelines are available in the Internet at https://www.baywa.com/fileadmin/media/relaunch/Downloads/Konzern/PRCC_BayWa_Code_of_Conduct_2015_deutsch.pdf.

Essentially, the risk management principles provide that risk management is to be complied with top-down through all hierarchical levels and that risk management and risk handling is a permanent task along with the operating processes:

As a rule, risks are not the consequence of wrong actions of the individual staff member.

Risk reporting should not be seen as self-reporting; it rather means to deal with any potential adverse impacts in the business area in due time in order to avoid unpleasant surprises.

2. *Scope of application and organisation of the risk management in BayWa AG*

BayWa AG's risk management system has a decentralised structure, i.e. each subsidiary/integrated affiliate, division and central organisational unit is responsible itself for carrying out for handling risk management (see figure in no. A4.). The responsibility includes both continuous updating and development of the risk management system and risk communication to the management of the division, or the manager or head of a central organisational unit.

Subsidiaries/affiliates are normally managed as an organisation with its own risk management.
Smaller subsidiaries/ affiliates may also be integrated in higher-ranking subsidiaries/ affiliates. The classification of the units is specified in Annex "B1 – Overview of subsidiaries/ integrated affiliates, divisions and central organisation units".

The subsidiaries/affiliates, divisions or central organisational units are responsible for ensuring that the risks are comprehensively identified, assessed, controlled and communicated; they are in particular responsible for ensuring that measures adopted to influence risks are actually implemented.

A risk owner has to be appointed for each subsidiary/ affiliate, division or central organisational unit. The risk owner is responsible for assessing the risk situation in his area of responsibility, for communicating the risks to higher hierarchical levels and for carrying out the ongoing risk control.

For the administration of the risk management, each subsidiary/ affiliate, division and central organisational unit has to appoint one risk manager, who introduces and explains the risk management system to the involved staff members. The risk manager's responsibilities further include identifying, classifying, evaluating and documenting the own risks in the risk management system R2C, reporting to the risk owner and the central risk management.

Corporate Controlling will request each year an update on the risk owners and managers. The names of the risk owner and the risk contact as well as any changes of the persons carrying out such functions are to be reported to the Corporate Controlling department on an ad-hoc basis (cc.planning@baywa.de).

Corporate Controlling is responsible for the central risk management. It performs the policy-making and coordinating functions within the risk management system, i.e. it is responsible for the following:

- standardising the risk documentation and communication
- determining the risk review schedules
- identifying and analysing the entire risk portfolio and aggregating the risk for the reporting to the management board
- contact for all questions as to the scope, principles, organisation and process of risk management

In case of questions concerning Risk Management with R2C please contact:

Thomas Oberstadler, Head of Corporate Controlling
089 / 9222 - 3590

Stephan Patij,
089 / 9222 – 3587

Sabine Reibenspies,
089 / 9222 - 2732

Steffen Glücks,
089 / 9222 - 3629

Josef Zeiler jun.,
089 / 9222 - 3211

3. Risk management process

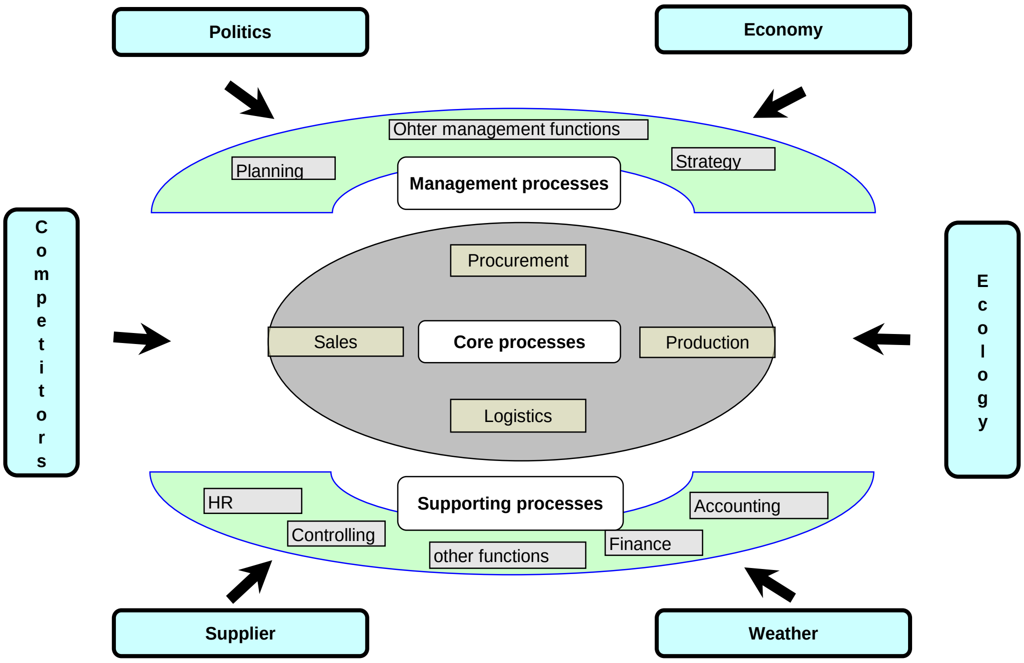
Corporate Controlling requests a complete review of the risk assessment on an annual basis and updates the risk management system accordingly where required. By doing so, it ensures that up-to-date data are available for potential external audits, for defining the thresholds and as an information basis for strategic planning.

In coordination with the auditors, it has been defined that newly identified risks and changes as to known risks are to be promptly included in the existing risk management in corporation with Corporate Controlling.

The risk management system documents the risks in the risk software R2C in detail for each subsidiary/affiliate, division and organisational unit carrying out its own risk management or central organisational unit. BayWa AG's risk database is available to the risk owners and managers for editing on the internet (http://www.risk-data.com).

3.1 Risk identification

The various, internal and external risk impacts on the Group are illustrated below.



For a better overview, the Group's risks are structured according to several aspects.

The risks are allocated to the following main categories:

Risk categories:

- Compliance risks
- Financial risks
- Strategic risks
- Operational risks
- Legal risks
- Structural - /Procedural Organization
- Market risks

The risk identification is carried out in R2C (risk to chance) and can be accessed either via the action menu under 'create risk' (new risk) or via the reporting cockpit (existing risks).

As a rule and as set forth in the German Act on Supervision and Transparency in Businesses, all risks that might threaten the continued existence of the enterprise must be recorded.

Beyond the legal term "risks threatening the continued existence of the enterprise", BayWa AG stipulates that all risks detected are to be included in the risk management system. To ensure the completeness of the risk inventory, there is no minimum risk recording level as to the value at risk.

The risk owner is to be specified in the risk identification. Such risk owner is the staff member within the subsidiary/affiliate, division or central organisational unit who is in charge of managing and handling the individual risk and who is directly responsible for the implementation of the applicable measures.

3.2 Risk analysis

The risk analysis is carried out in R2C in the risk statistic and/ or the underlying, corresponding detailed information for each risk.

[Impact]					
catastrophical	2 / -	4 / -	1 / -	- / -	- / -
critical	7 / -	20 / -	12 / -	3 / -	1 / -
noticable	6 / -	10 / -	24 / -	4 / -	- / -
small	22 / -	33 / -	39 / -	9 / -	3 / -
very small	24 / -	16 / -	8 / -	- / -	- / -
	very low	low	medium	high	very high
[Likelihood]					

The intervals of the probabilities of occurrence are defined as follows:

Brief description	Abbreviation	Label
very low	1	0 % < likelyhood <= 5 %
low	2	5 % < likelyhood <= 10 %
medium	3	10 % < likelyhood <= 20 %
high	4	20 % < likelyhood <= 50 %
very high	5	50 % < likelyhood <= 100 %

The above verbal, qualitative evaluations do not correspond to unambiguously defined mathematical values.

As a rule, the amount of damage or loss is to be assessed as a net amount, i.e. after measures to avoid, reduce or transfer the risk have been taken.

A plausible or realistic worst case is to be applied as a reference for quantifying the potential damage or loss.

As the value at risk, always the impact on the results is to be recorded in the risk record form. Such impact on results will normally be determined based on the factors "turnover", "earnings" and "cost".

The “Risk analysis” section documents the calculation process and/or how the amount of the individual risk’s impact on results has been determined. It has to be borne in mind that the risk analysis by all means has to describe in detail and comprehensibly how the amount of damage or loss has been determined. Where possible, an example calculation or a reference to a past event should be provided. Cost adjustment potential is to be taken into account in determining the amount of damage or loss. It makes also sense to provide a damage scenario including the assumptions made.
In such scenarios, corrective action as to costs is also to be taken into account.
Subjective estimates suffice only in exceptional cases.

3.3 Risk communication

The risk communication consists of the oral and written reporting within the enterprise’s hierarchical organisation.

Risk communication includes the individual reporting system for each risk and the defined organisation.

Existence-threatening risks in all subsidiaries/affiliates, divisions and organisational units are reported once a year to the overall management board by Corporate Controlling.

Each subsidiary/affiliate, division and organisational unit reports independently in line with the handling instructions applicable to the respective subsidiary/affiliate, division and organisational unit ensuring the information flow to the management of the division or the head of the central organisational unit, as applicable, and simultaneously to Corporate Controlling, Mr Oberstadler.

The complete chain of communication is to be recorded in R2C on the third page of the ‘risk creation’ dialogue.

3.4 Risk control and documentation

The identified and evaluated risks are controlled at this stage by the applicable risk owner (decision maker for the individual risk); in individual cases, such control may consist in accepting the risk, but also in reducing, transferring (insurance) or completely avoiding it by way of suitable measures.
In most cases, it will consequently be required to specify the measures.
In doing so, it is required to fully illustrate the measures

Such control by way of measures requires that an internal control system is actively carried out, but also that an early-warning system is integrated and an emergency plan is developed.

All agreed measures to handle the individual risk are to be documented in R2C within the ‘action-definition’ dialogue for the respective risk.

In addition to the effectiveness of the measures, the risk owner and the costs associated with the implementation of the measure (cost-benefit calculation) are to be recorded.

All policies and measures as to early-warning systems and emergency plans made or taken in connection with the handling of this risk are to be recorded under documentation.

Such documentation is intended to sufficiently record the intended risk management activities in each subsidiary/affiliate, division and organisational unit with respect to each individual risk; it is also intended to provide proof to external and internal auditors that the risk management is in place and being carried out.

The individual documents are based in particular on the developed and adopted strategies and measures and on the defined methods of communicating and handling the respective risk.

Archive paths to the documented instructions, policies and definitions will facilitate the day-to-day work with the individual risk and the entire risk management. The specified documents should be archived with the relevant risk contact. R2C offers the possibility to upload relevant documents to the respective risk.

3.5 Risk monitoring

The annual re-assessment of the risks in the R2C is not only intended to identify all significant and existence-threatening risks, but also to monitor the risks already identified. When carrying out the update, the risk manager is able to assess whether the risk is controlled by way of the adopted strategies and measures in a way that is in line with BayWa AG's risk management principles.

Where this is not the case, the risk manager has to analyse the deviations and communicate them to the risk owner to take appropriate corrective action.

4. Supervision of the risk management system

Such supervision consists of monitoring the risks and the risk management system and of reviewing the risk management system and the identified risks.

4.1 Monitoring the risks and the risk management system

Such monitoring is to be performed by the affected risk owner or risk holder, i.e. subsidiary/affiliate, division or organisational unit, and relates to the monitoring of an internal control system (ICS).

This task consists essentially of the ongoing maintenance and updating of the risks and the entire risk management system.

It includes in particular the monitoring of the risk contents and the implementation of the adopted strategies and measures including comprehensive documentation.

4.2 Reviewing the risk management system and the risks

The review of the risk management system and the realisation of the ICS-controlsis performed by external auditors and/ or the internal audit department.

Within their scope of the mandate to audit the annual accounts, the external auditors will also audit the risk management as to an appropriate installation of the system and an appropriate internal audit function.

This will include also a review as to whether the necessary measures have been taken in an appropriate manner and whether the installed monitoring system is able to perform its functions.

The Internal Audit department reviews the central risk management as well as the risk management system installed in the subsidiaries/affiliates, divisions or organisational units.
The selection of subsidiaries/affiliates, divisions or organisational units being reviewed takes place in cooperation with the central risk management as well as by considering the significant risks.

5. Instruments of the ongoing risk monitoring and control

ICS
Internal control systems are in place in the subsidiaries/affiliates, division or organisational units for various processes, ensuring permanent monitoring of the risks. These processes are, where possible and reasonable, IT-supported processes.

Riskboard
Another instrument of ongoing risk monitoring and control is the Riskboard held every two to three weeks at the highest level of the Group.
The Riskboard is attended by the Management Board, the assistant to the Management Board, Corporate Finance, Corporate Controlling, Internal Audit, Corporate Legal, Compliance, Corporate Governance, Investor Relations, Insurance, Corporate Business Development, Corporate Marketing, PR & Corporate Communications, BayWa Services, CREM, Corporate HR, EH&S, Corporate Sustainibility, Corporate Risk, CEO BAST, CFO BAST, COO BAST, Head of Agricultural Products, Commercial Trading of Agricultural Products, Business Development Agricultural Products, Head of Agricultural Equipment, Head of Special Agricultural Equipment, Head of CLAAS-subsidiaries, Controlling Agricultural Products, Head of Business Development Agri-Services, Head of Energy, Business Development Energy, Head of Building Materials, Controlling ABT, COO ABT, General Manager Fruit, Management of the BayWa r.e. group, CEO and COO RI-Solution, Head of Corporate IT-Security, Head of BayWa Stiftung.

All units present their risk situation in relation to the current business development. Following discussions on the risk situations, corrective measures are adopted where required.

Business Review
Business Reviews are conducted on a quarterly basis to assess the current development of business as well as the current opportunity and risk situation.

Annexes

Annex A1	-	German Act on Supervision and Transparency in Businesses
Annex A2	-	Section 91 of the German Stock Corporation Act
Annex B1	-	Overview of subsidiaries/ integrated affiliates, divisions and central organisation units