



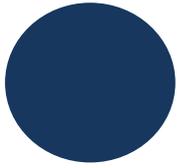
Risk Manager

The Risk Manager Framework

A professional Reference Tool



80 Boulevard Haussmann F-75008 PARIS



Foreword

The profession of Risk Manager is moving forward, undergoing changes and developing within our companies, both in France and on an international level.

In order to further the awareness, the technical skills and the added value of the Risk Manager's profession, it was indispensable to construct a professional reference tool – a real framework for understanding the activities, the tasks and the skills embodied in the Risk Manager.

The AMRAE takes pleasure in presenting you with the **first Risk Manager's Professional Reference Tool**, the fruit of our 10 years' experience in further education, of our bi-annual surveys of the Risk Manager's position and of our members' exchange of professional experience.

Within the pages of this document, we bear witness to the outlines, the activities and the contribution of the position, as well as to the commitment of the Risk Manager alongside General Management to helping in choosing beneficial risks and the way they are financed.

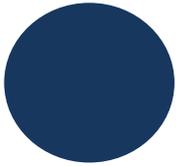
We entrust to further education the key to success for future generations. We share our vision of the profession with **various countries, both in Europe and beyond**.

We wish to address our warm thanks to the working-group, which, under the guidance of François Malan, the Nexity Risk Manager, has produced this consummate finished product.

We have a firm belief in our commitment and in our added value for our organisations.

Gilbert Canaméras

Chairman AMRAE



Contents

General Presentation of the AMRAE Reference Tool	6
Caution.....	6
Risk Management.....	7
The Risk Manager	7
Qualities & Skills	8
The Professional Reference Tool	10
Activities / Tasks.....	
Requirements / Qualities & Skills	
Appendix: Glossary for The AMRAE Risk Manager's Professional Reference Tool.....	28
Thanks	37



General presentation of the AMRAE Reference Tool

Since 2010, the AMRAE has been working towards the definition of a Risk Manager's professional reference tool.

At the same time, FERMA wishes to promote proper recognition of the profession and its specific aspects, by means of a skill accreditation project, based on a reference tool highlighting the person practicing this profession (and not the Risk Management arrangements).

As the Risk Managers' professional association, the AMRAE elaborates its own vision of the profession, by drawing up an inventory of the tasks that are essential for the achievement of its missions, together with the skills and qualities that enable success in the position.

The AMRAE has at its disposal both assets and essential tools for the reflection process:

- Over 10 years, "AMRAE Formation" has been putting together numerous further education courses dealing with the missions associated with the Risk Manager and imparting the necessary skills.
- The three editions of the Risk Manager Barometer (2009-2011-2013) have enabled precious indications to be provided as to the missions, profile, compensation and future of the profession.
- The AMRAE members' returns on experience and discussion themes provide up-to-date knowledge of the know-how, requirements and skills inherent to their profession.

Caution

The aim of the reference tool built up by the AMRAE is to present the widest possible overview of the Risk Manager's activities. Despite this, it should not be taken as a model to be systematically applied as a whole.

The Risk Manager is liable to be confronted with all the activities listed in the reference tool but depending on the organisation and the missions with which he is entrusted, he may be required to act in all these areas or only in some of them.

The AMRAE may be led to revise its reference tool so as to incorporate the future evolutions and stakes of the profession of Risk Manager.



Risk Management

Definition¹

Risk management concerns all the actors in a company. Its aim is to be all-encompassing and it must cover the entire activities, processes and assets of the company

Risk management is a dynamic system within the company, defined and implemented under its responsibility.

Risk management comprises a set of means, **behaviour**, procedures and actions attuned to the characteristics of each company, enabling management to keep risks at a level that is acceptable for the company.

Risk denotes the possibility that an event may occur, the consequences of which would be liable to be detrimental to the staff, assets, environment and objectives of the company or to its reputation.

The aims of risk management:

- To create and preserve the value, assets and reputation of the company.
- To safeguard decision-making and processes within the company in order to facilitate the achievement of its objectives
- To encourage coherence between the company's actions and its values
- To mobilise the company's staff behind a shared vision of the main risks



The Risk Manager

Depending on the organisation, the Risk Manager takes responsibility for all or part of Risk management, which comprises the following activities:

- Definition of the arrangements' missions and structure
- Risk appraisal (risk identification, analysis, evaluation)
- Risk control (to an acceptable level, function of the chosen risk criteria)
- Dissemination of risk culture
- Risk financing in line with the risk management policy
- Handling uninsured or uninsurable events
- Claims handling
- Crisis management
- Steering and Reporting

He submits to General Management the organisation's risks and optimised financing solutions, thus enabling acceptable limits to its risk-taking to be laid down, together with the control of such risks.

¹The AMF's* reference framework: Risk Management and internal control mechanisms (* Autorité des Marchés Financiers, the French Financial Markets Authority)



Organisation

Capable of:

- Rigorously shaping his position, so as to perform his activities efficiently
 - Defining clear and precise action plan and objectives
 - Prioritisation and planning of actions
- Ascertaining the execution of delegated tasks

Management

Capable of:

- Team mobilisation and support
- Giving precise indications, having a clear vision
- Stimulating the buy-in of various parties: General Management, the organisation's departments, teams, correspondents
- Encouraging relationships of trust and convergence around commonly accepted objectives

Receptiveness

Capable of:

- Being attentive and listening to those who are talking to him
- Detecting weak signals
- Remaining objective, keeping an open and unprejudiced mind

Communication

Capable of:

- Maintaining appropriate behaviour and speech, encouraging dialogue and relationships of trust
- Easy, clear and convincing written and oral expression
- Showing qualities of leadership
- Understanding the person to whom he is speaking, negotiating whilst showing a degree of diplomacy
- Sharing information in a transparent manner, whilst maintaining the necessary confidentiality
- Negotiating in the best interests of the organisation

Creativity and Adaptability

Capable of:

- Modifying actions in the light of a changing context
- Adapting his language depending on the person to whom he is speaking
- Bringing change to his organisation so as to improve it and bring it into line with the organisation's overall objectives and external influences, regulatory in particular.
- Thinking the unthinkable
- Putting forward novel approaches and viewpoints
- Creating innovative organisations and tools

Culture and awareness of what is at stake

Capable of:

- Having an overall understanding of the macro issues (economic, financial...), the environment (competition...)
- Understanding what is at stake, the various business segments and markets of the organisation
- Having a grasp of the culture and environment of the countries where the company is present and those which are important for its future
- Appropriating the organisation's values

Resistance to stress

Capable of:

- Objective analysis, deciding on efficacious actions, in high-pressure situations
- Accepting criticism and calling himself into question

TASKS

-
- Definition of the missions allocated to the risk management arrangements within the framework of the implementation of the strategy

-
- Assimilation of the threats and opportunities inherent to the strategy

-
- Identification of activities, processes (business segment, support)

-
- Development of the risk management organisational framework

ACTIVITY

Definition of the missions and structure of the arrangements

1

-
- Construction of the risk management methodology & reference tool

-
- Development of the risk management policy, taking into account the risk appetite and acceptance of General Management and/or of the organisation's bodies of Governance

-
- Obtaining approval of the arrangements' missions and structure from General Management and/or the bodies of Governance, as well as the allocation of the means required for their execution

REQUIREMENTS

QUALITY/SKILLS

Assimilation of the culture, history and specific aspects of the organisation and its context (competitive...)	<ul style="list-style-type: none"> • Organisation
Allocate objectives to the risk management arrangements and highlight their benefits	<ul style="list-style-type: none"> • Receptiveness
Obtain approval of the objectives from the organisation's bodies of Governance and make them known (first and foremost to the stakeholders in the risk management arrangements)	
As required, intervene within bodies responsible for defining strategy	<ul style="list-style-type: none"> • Culture and stakes
Provide methodological support in the identification and evaluation of risks linked to new strategic orientations	<ul style="list-style-type: none"> • Creativity and Adaptability
Assimilation of the stakes and constraints of the business segments, as well as their objectives	<ul style="list-style-type: none"> • Organisation
Knowledge of the business segments' functions and organisation charts	
Identification of the roles and responsibilities of the company's employees	
Definition of a target organisation enabling the specified objectives to be attained	<ul style="list-style-type: none"> • Organisation
Definition within an operational charter – foundation for the target structure - of the target organisation's profiles, roles and responsibilities; communicate to those involved (General & other managers, correspondents...)	<ul style="list-style-type: none"> • Creativity and Adaptability
Definition of means: human resources, IT, appropriate financial means	<ul style="list-style-type: none"> • Culture and stakes
Set up one (or more) risk committee(s)	
Define and organise relations with the internal control structure	
Define relations with Internal Audit	
Put together the reporting component items in line with the needs of the stakeholders	
Select a reference tool and, if necessary, adapt it as required by the specific aspects of the organisation	<ul style="list-style-type: none"> • Organisation
Define the implementation method	
Assemble the organisation's strategic objectives, broken down into operational objectives.	<ul style="list-style-type: none"> • Receptiveness
Define the object, the objectives and the scope (activities taken into account) of the risk management policy	<ul style="list-style-type: none"> • Culture and stakes
Define the main principles guiding risk control for the organisation (acceptance, avoidance, reduction, financing...)	<ul style="list-style-type: none"> • Communication
Define and implement the risk-financing strategy (self-insurance, transfer....)	
Define what are the acceptable limits of risk for the organisation.	
Obtain General Management's approval of the four preceding requirements	
Formalise the four preceding requirements in a risk management policy to be communicated to those concerned (Board Members, General Management)	
Compile and present the missions, structures and means that have been defined	<ul style="list-style-type: none"> • Management
Be convincing with regard to the added value of such defined missions, structures and means	<ul style="list-style-type: none"> • Communication

TASKS

- Definition of the necessary tools for risk assessment (benchmarks, interview guide, risk register and universe, common language...)

ACTIVITY

Risk assessment (Risk identification, analysis and evaluation)

2

-
- Early warning of risks and of their evolution (in conjunction with economic intelligence)

-
- Conducting individual interviews with senior executives and other managers

-
- Workshop facilitation for risk identification, analysis and evaluation (prioritization)

-
- Development of risk cartographies by unit/business segment or by major project

-
- Compilation and consolidation of the organisation's major risks

REQUIREMENTS

QUALITIES / SKILLS

Establish a risk universe for the organisation	• Organisation
Establish a graduation of the potential consequences in the event of a risk being realised and a graduation of risk occurrence	• Creativity and Adaptability
Define and make use of a common language (glossary...), make it known within the organisation	• Receptiveness Ability to listen
Clarify, where necessary, the difference between raw and residual risks	
Select the appropriate medium and draw up a risk register	
Develop an interview guide and communicate it to those concerned	
Define the specific reporting formats and frequencies for the risk management arrangements	
Validate the appropriate tools for risk appraisal by stakeholders	
Make the arrangements' tools known to Internal Audit	
Draw up an inventory of the processes within the organisation's activities for strategic watch, business and regulatory intelligence	• Receptiveness Ability to listen
Provide input for the strategic watch by means of appropriate information gathered whilst on missions	• Organisation
Analyse weak signals	
Incorporate relevant weak signals in risk appraisal	
Identify risks, their causes and their impact	• Resistance to stress
Encourage their disclosure and identify both opportunities and threats	• Receptiveness
Establish and underpin risk assessment, on a raw and/or residual basis	
Once the exchange of views has taken place, clarify, summarise and restate these exchanges	• Communication
Update and make use of the arrangements' tools	
Lead, facilitate a group of senior executives, managers and, if necessary, experts	• Communication
Encourage the identification of opportunities as well as threats	• Receptiveness
Identify risks, their causes and their impact	
Assess risks on a raw and/or residual basis	• Resistance to stress
Clarify, summarise and restate these exchanges	
Establish a matrix attuned to the organisation and the needs of each entity/business segment or of the project concerned	• Organisation
Update & keep a record of risk cartographies	• Management
Organise risk feedback from the entities concerned	
Challenge the risks identified in the various entities – Analyse potential correlation	• Organisation
Consolidate retained risks	• Management
Provide the consolidated risk cartography to stakeholders	

TASKS

-
- Presentation / Validation of major risks

-
- Identification of the full range of available risk treatment measures

-
- Participation in drafting action plans

ACTIVITY

Risk control (to an acceptable level, function of the chosen risk criteria)

3

-
- Analysis and deployment of risk treatment action plans

-
- Assistance in acquisition and sale audits

-
- Visiting hazardous areas

-
- Consolidation and follow-up of action plans

REQUIREMENTS

QUALITIES / SKILLS

Compile summary of risks held to be major and submit it to General Management	<ul style="list-style-type: none"> • Organisation
Obtain validation of priorities in dealing with major risks	<ul style="list-style-type: none"> • Receptiveness
Obtain the designation of an owner for each major risk	
Draw up an inventory of the operational methods of dealing with a given risk (construction, training...)	<ul style="list-style-type: none"> • Organisation
Draw up an inventory of risk financing programmes (insurance, "captives" ...)	<ul style="list-style-type: none"> • Management
Draw up an inventory of internal control activities	
Draw up an inventory of Business Continuity Plans and ensure they are tested	
Draw up an inventory of crisis management plans and ensure they are tested	
Define the criteria against which the aforementioned risk treatment tools are judged	
Suggest further risk treatment solutions in addition to those of the risk owner	<ul style="list-style-type: none"> • Culture and stakes
Participate in drawing up business continuity plans	<ul style="list-style-type: none"> • Creativity and Adaptability
Participate in drawing up risk prevention plans	
Carry out risk diagnoses, in conjunction with the appropriate specialists (internal, and where necessary, external experts) and follow up insurers' recommendations	<ul style="list-style-type: none"> • Organisation • Management
Carry out training and actions to improve awareness (road safety, expats...)	
Have the treatment validated by the other "support" functions concerned	
Define jointly, with each risk owner, a timetable for the implementation of the action plan	
Identify risk areas	<ul style="list-style-type: none"> • Receptiveness
Establish treatment plans in the light of the criticality of the risk areas and the organisation's risk appetite	<ul style="list-style-type: none"> • Creativity
Highlight potential risks which may endanger the completion of the acquisition or sale	<ul style="list-style-type: none"> • Receptiveness
Identify and evaluate post-acquisition or -sale risks	<ul style="list-style-type: none"> • Creativity
Suggest appropriate risk treatment measures	
Align insurance or self-insurance coverage with the involvement of the future operation	<ul style="list-style-type: none"> • Management
Have oneself accompanied by appropriate specialists (internal and, where necessary, external experts)	<ul style="list-style-type: none"> • Communication
Give advice in respect of the obvious immediate operational actions	
Meet risk correspondents or those in charge of risk areas	
Draw up actions and budgets, risk by risk	<ul style="list-style-type: none"> • Organisation
Support the implementation of risk treatment measures decided by the risk owner	
Present the consolidated action plans to stakeholders	<ul style="list-style-type: none"> • Communication • Resistance to stress

ACTIVITY

Dissemination of risk culture

4

TASKS

-
- Developing, leading, training a network of risk correspondents
-
- Participating in important events (seminars, committees...)
-
- Drafting internal communications concerning risk culture

REQUIREMENTS

QUALITIES / SKILLS

Disseminate risk culture in accordance with the defined policy

- Communication

Train correspondents in methodology, their role and the way risk management works

Organise sharing amongst correspondents of best practices and return on experience

- Management

Participate and, where appropriate, play a role in these events and communicate on risk culture, on measures for dealing with major risks ...

- Communication

Encourage return on experience from the field

Using a few simple explanations, clarify the components of risk culture (actions carried out, return on experience, deployment timetable...)

- Communication

Distribute this communication using multiple internal channels

- Management

Deploy risk culture in accordance with the defined policy

Train correspondents in the methodology, their role and the way risk management works

TASKS

- Inventory of risk-financing solutions

-
- Organising relations with service providers (brokers, insurers)

-
- Negotiating insurance contracts

-
- Administration and deployment of insurance coverage

-
- Setting-up and management of a captive

ACTIVITY

Risk financing
in accordance with policy

5

REQUIREMENTS

QUALITIES / SKILLS

Seek out available solutions corresponding to the organisation (Insurance, internal financing "self-insurance" or alternative systems, amongst which all the various types of captive solutions available on the market)	<ul style="list-style-type: none"> • Culture and stakes
Ensure monitoring and benchmarking of the market for risk-financing solutions (insurance companies, banks, financial markets)	<ul style="list-style-type: none"> • Creativity Adaptability
Define the resources linked to these solutions, draw up a comparison of the advantages /disadvantages	<ul style="list-style-type: none"> • Organisation
Define the criteria for selection of service providers	
Obtain validation of the various points put forward: model, resources, selection criteria	
Identify potential service providers	<ul style="list-style-type: none"> • Organisation
Define the contractual terms for each service-provider, in accordance with professional rules and practices, paying particular attention to the roles of each party and their remuneration – Define the criteria for performance measurement	<ul style="list-style-type: none"> • Communication
Negotiate and formalise the service provision contract with the broker	
Analyse the insurance proposal (limits, policy excesses...) in conjunction with the organisation's identified requirements (insured sums and cover) / define the policy forms	<ul style="list-style-type: none"> • Resistance to stress
Define the main contractual clauses and the criteria for performance measurement	<ul style="list-style-type: none"> • Receptiveness Ability to listen
Have the insurance contracts drafted / validated by the broker	
Disseminate within the organisation information concerning the cover (contents, exclusions...)	<ul style="list-style-type: none"> • Organisation
Monitor premium payments, contract renewals, any renegotiation	<ul style="list-style-type: none"> • Management
Organise a follow-up of the performance criteria	<ul style="list-style-type: none"> • Communication
Annual consolidation of results (claims experience, policy costs, shortcomings, cover...) and report to internal decision-makers and the various actors concerned (both internal and external)	
Adapt cover to the evolution of risks and to required insured sums	
Analyse the benefit, the objectives and the feasibility of a "captive"	<ul style="list-style-type: none"> • Culture and stakes
Select the partners (actuary, manager...) and organise the implementation of the "captive"	<ul style="list-style-type: none"> • Organisation
Participate in the management of the "captive"	
Comply with the regulations and communication associated with the "captive"	

ACTIVITY

Handling uninsured / uninsurable events

6

TASKS

-
- Categorising the event
-
- Identifying and taking account of the means and action plans
-
- Organisation of return on experience

REQUIREMENTS

QUALITIES / SKILLS

Define the scope, the stakes, the consequences...

Collect information from stakeholders

Where appropriate, implement the means and action plans

Verify that the means and action plans are consistent with those expected

Identify occurrences of similar events within the organisation

Identify the triggers

Where appropriate, inform the bodies of Governance

Where appropriate, update the cartography and/or the action plan

- Organisation
- Receptiveness Ability to listen
- Organisation
- Resistance to stress
- Receptiveness and ability to listen
- Communication

TASKS

- Categorising events in order to determine applicable coverage and potential liability

-
- Management organisation in collaboration with partners (brokers, insurers, loss adjusters, even reinsurers...)

-
- Claims follow-up

-
- Ratification of return to normal activities

ACTIVITY

Claims handling

7

REQUIREMENTS

QUALITIES / SKILLS

Obtain information concerning events	• Communication
Pass the information collected to bodies of Governance with a view to internal and/or external communication	• Organisation
Check that the insurance policy can be activated	• Management
Trigger the crisis response, business continuity and business resumption procedures (or ensure that they have been triggered)	• Resistance to stress
Validate with the owner of the risk that has occurred the nature and impact of the events	
Analyse the causes of the loss and its consequences in terms of financial and reputational impact, check the quality of the information provided.	
Examine the possibility of recourse against liable third parties	
Submit the claim or check that the claim submittal clauses are complied with (conditions and form of the claim)	• Organisation
Exchange information with partners in order to validate the categorisation of the event, the quantum of loss, the conditions applicable to the loss indemnification, the methods for the administration of the plan	• Resistance to stress
Define the administrative actions and corrective measures	• Management
Identify the loss adjusters' missions, negotiate the conditions for the follow-up (timing, cost) and monitor the actions by means of regular reporting.	
Supervise the follow-up of the claims handling plan, in particular by means of regular reporting from those involved, both internally and externally (partners)	• Organisation
Ensure that the claim has actually been settled	• Management
Provide regular information to General Management and ensure that internal and external communication is both relevant (in accordance with the strategy defined by the organisation) and up-to-date.	• Communication
Check with partners and key internal actors the validity of the return to normal activity	• Organisation
Analyse the performance of partners against the performance criteria and the expected results	• Communication
Define corrective actions so as to avoid the occurrence of a similar loss (draw conclusions in terms of the types of cover and the insured sums taken out)	
Put together and disseminate within the organisation a return on experience	

TASKS

- Contribute to the definition, implementation and communication concerning the organisation, and the prevention and crisis management tools
-

- Assistance in crisis management
-

- Maintenance and continuous improvement of the crisis management arrangements

ACTIVITY

Crisis management

8

REQUIREMENTS

QUALITIES / SKILLS

Contribute to defining what is a crisis and how it is evaluated	• Receptiveness Ability to listen
Contribute to defining warning systems	
Participate in identifying those to be involved in the crisis response team, their roles and responsibilities, and contribute to the definition of the practical aspects of the crisis response team's activity	• Culture and stakes
Contribute to the communication on the crisis response unit	• Resistance to stress
Contribute to mobilising those involved in the crisis response unit and the coordination of its proceedings	• Organisation
Submit to the crisis response team the decision as to whether to activate the Business Continuity Plan or not	• Resistance to stress
As the case may be, keep the files / archives of the crisis	• Management
Check the leader assumes his roles and responsibilities	
Participate in coordinating the required training /simulation exercises	• Management
Ensure that the procedures are updated	
Capitalise on the return on experience	• Communication

TASKS

-
- Continuous maintenance of, and improvement to the risk management arrangements

-
- Facilitation of the risk committee

-
- Reporting to the arrangements' stakeholders

-
- External communication

-
- Organisation of relations with internal audit

ACTIVITY

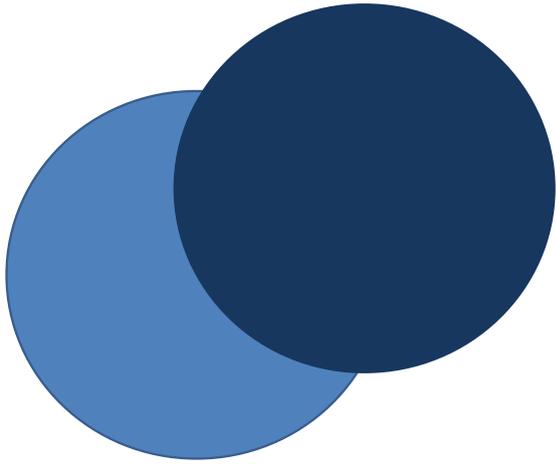
Steering and Reporting

9

REQUIREMENTS

QUALITIES / SKILLS

Act as the driving force behind the arrangements	<ul style="list-style-type: none">• Culture and stakes
Establish and disseminate risk-monitoring dashboards, together with an assessment of the risk management activities and their efficacy	<ul style="list-style-type: none">• Creativity and adaptability
Define and apply risk-monitoring indicators and those for the implementation of the risk management arrangements	<ul style="list-style-type: none">• Organisation
Identify participants in the risk committee(s): define the role and operating procedures of the risk committee(s)	<ul style="list-style-type: none">• Communication
Facilitate the committee(s), prepare the agenda and plan forward for arbitrations	<ul style="list-style-type: none">• Receptiveness and ability to listen
Define with stakeholders the arrangements' format and operating procedures	<ul style="list-style-type: none">• Communication
Present to stakeholders the arrangements' deliverables (cartography, follow-up of action plans, analyses, indicators...)	<ul style="list-style-type: none">• Resistance to stress
Present information on the organisation's risks to those in charge of financial communication	<ul style="list-style-type: none">• Communication
Execution of deliverables for supervisory authorities, drafting the "risk factors" section in the reference document	<ul style="list-style-type: none">• Organisation
Participate in drawing up the audit plan	<ul style="list-style-type: none">• Receptiveness and ability to listen
Gather information useful for risk management (new risks, evaluation...)	



APPENDIX

Glossary : AMRAE Reference Tool – Profession Risk Manager



AMRAE Reference Tool – Profession Risk Manager

Bottom-Up Approach²

Process for the **identification** and **evaluation of risks** within entities, Business Units, areas... consolidated at Corporate level. This process can be based on existing risk management procedures, such as the analysis of regulatory risks, and beneficially enriched by an analysis of operational risks. This process enables the involvement of the various operational levels and their corresponding risks, with which the hierarchy is often not completely familiar, and facilitates the implementation of concrete action plans so as to consolidate the results. This process can be carried out in addition to the **Top-Down approach**.

Captive³

- ✓ Captive insurance company: an insurance company which is owned, either by a financial company, other than an insurance or reinsurance company or group of insurance or reinsurance companies (within the meaning of article 212, paragraph 1, point c of the Directive 2009/138 referred to above), or by a non-financial company, and whose object is to provide insurance cover concerning exclusively the **risks** of the company or companies by which it is owned or alternatively the **risks** of one or more other companies belonging to the group of which it is part.
- ✓ Captive reinsurance company: a reinsurance company which is owned, either by a financial company, other than an insurance or reinsurance company or group of insurance or reinsurance companies (within the meaning of article 212, paragraph 1, point c of the Directive 2009/138 referred to above), or by a non-financial company, and whose object is to provide reinsurance cover concerning exclusively the **risks** of the company or companies by which it is owned or alternatively the **risks** of one or more other companies belonging to the group of which it is part.

Consequence⁴

The result of an event impacting objectives

Note 1 One **event** can give rise to a series of consequences.

Note 2 A consequence may be certain or uncertain and may have a positive or negative impact on the achievement of objectives.

Note 3 Consequences may be expressed in qualitative or quantitative terms.

Note 4 Initial consequences may set off chain reactions.

Entity

Department or subsidiary of the **Organisation**

² Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

³ Definitions from Directive 2009/138/CE of the European Parliament and Council of November 25th 2009 concerning the taking-up and pursuit of the business of insurance and reinsurance

⁴ Reference : Iso 31000

External Context⁵

Outside environment within which the organisation seeks to attain its objectives

Note The external context can comprise:

- ✓ the cultural, historical, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, at an international, national, regional or local level,
- ✓ the factors and trends having a significant impact on the **organisation's** objectives, and
- ✓ the relationships with external **stakeholders** , their views and their values.

Governance of the organisation

General Management, Board of Directors or Supervisory Board, Assemblies of elected representatives,

Internal Audit⁶

An independent and objective function providing the **organisation** with assurance in respect of the level of control of its operations, giving advice for their improvement, and contributing to the creation of added value.

Internal audit assists the **organisation** in achieving its objectives by evaluating its **risk management**, control and corporate governance procedures, using a systematic and methodical approach, and by submitting proposals with a view to reinforcing their effectiveness.

Because of the variety of areas to be covered and the missions to be carried out, internal audit needs to have at its disposal an ever-widening skill-set. On-going training constitutes a key performance factor, both individually and collectively.

Internal Context⁷

The internal environment within which the **organisation** seeks to attain its objectives

Note The internal context can comprise

- ✓ the governance, the organisation, roles and responsibilities,
- ✓ the policies, the objectives and the strategies put in place to achieve the latter,
- ✓ the capabilities, in terms of resources and knowledge (for example, capital, time, staff, processes, systems and technologies...),
- ✓ the information systems, information flows and the decision-making processes (both on a formal and informal level),
- ✓ the relations with internal stakeholders, as well as their views and values,
- ✓ the organisation's culture,
- ✓ the standards, guidelines and models adopted by the **organisation**, and
- ✓ the shape and extent of contractual relations.

Internal Control⁸

A mechanism of the organisation, defined and implemented under its responsibility, comprising a set of means, behaviour, procedures and actions attuned to the specific characteristics of each organisation, which:

- ✓ contributes to the control of its activities, to the efficacy of its operations and the efficient use of its resources, and
- ✓ must enable it to take appropriate account of significant risks, whether they be operational, financial or those of compliance

⁵ Definition taken from Iso 31000 including modifications

⁶ Definition of the French Audit and Internal Control Institute

⁷ Definition taken from Iso 31000 including modifications

⁸ Definition taken from the AMF* reference framework (posted on line July 22nd 2010): Risk management and internal control arrangements (* Autorité des Marchés Financiers, the French Financial Markets Authority)

More particularly, the mechanism's aim is to ensure:

- ✓ compliance with laws and regulations;
- ✓ that the instructions and guidelines laid down by General Management or the Board are applied;
- ✓ the correct functioning of the organisation's internal processes, in particular those contributing to the safeguarding of its assets;
- ✓ the reliability of its financial information

Level of risk⁹

Outcome of a risk evaluation taking into account its criticality and its control. The result can be broken down into the level of **raw risk**, level of **residual risk** and level of target residual risk.

Major Risk

A risk, the consequences of which and probability of realisation are extremely important for the **organisation**.

Monitoring¹⁰

Checking, supervision, critical observation or assessment of the status with a view to continual identification of modifications compared to the required or expected performance level

NOTE Monitoring can be applied to a **risk management organisational framework**, to a **risk management process**, to a **risk** or to a method of **risk** control.

Organisation

The organisation is the company or public body concerned

Raw Risk¹¹

A risk before any prevention and protection measures have been taken into account. Generally, operational risks are analysed on a raw risk basis, so as to identify, evaluate and test which treatment methods have been put in place to control the risk.

Residual Risk¹²

Risk remaining after risk treatment

A residual risk may include an unidentified risk.

The residual risk can also be called "net risk"

Risk

Prior perception of an event, the consequences of which, should it occur, would be liable to prevent the achievement of an objective or would constitute an opportunity for the **organisation**.

Risk Analysis¹³

A process put in place so as to understand the nature of a **risk** and to determine the **level of risk**

Note 1 The **risk** analysis provides the basis for the **risk evaluation** and the decisions concerning the **risk treatment**.

Note 2 The **risk** analysis includes the **risk** estimation.

⁹ Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

¹⁰ Reference : Iso 31000

¹¹ Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management" including modifications

¹² Definition taken from Iso 31000 including modifications

¹³ Reference : Iso 31000

Risk Appetite¹⁴

Level of risk to which the **organisation** is prepared to expose itself within the framework of its mission or vision

Risk Assessment¹⁵

The complete process of risk identification, risk analysis, and risk evaluation

Risk Cartography¹⁶

Summarised and overall view of **risks**, prioritised according to the **organisation's** criteria. It enables an inventory to be drawn up at a given moment of the various risks that the company or the group would be able to bear or already bears.

Risk Committee

A committee made up, depending on the organisation, of representatives of operational management, decision-making bodies and/or experts whose mission (which can vary from one organisation to another) can be to identify risks, to follow up risk control action plans, to present to governance bodies the risk status.

Risk Correspondents¹⁷

Members of the risk sphere responsible on a local level within each entity, and under the authority of the Risk Manager, for being the driving force behind the **risk management** process

They participate in the proceedings for drawing up the **risk cartography**, inform the Risk Manager of the occurrence of significant new **risks** and assist **risk owners** in the preparation of action plans.

Risk Criteria¹⁸

Reference terms enabling the assessment of **risk** importance. Risk criteria can include risks and benefits, legal and regulatory requirements, social, economic and environmental dimensions, **stakeholders'** concerns, priorities and other assessment criteria.

Risk Evaluation¹⁹

Implementation of an evaluation method reflecting the organisation's culture and allowing prioritisation and comparison of the **risk analysis's** results with **risk criteria** so as to ascertain whether the **risk** and/or its intensity are acceptable or tolerable

Risk evaluation helps in the decision-making linked to **risk treatment**.

Risk Financing²⁰

Mechanism, the aim of which is to have all or part of the risk borne by an outside third party (insurance, captive...). The term can also designate provisions intended to cover the costs of implementing risk treatment.

¹⁴ Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

¹⁵ Reference : Iso 31000

¹⁶ Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

¹⁷ Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

¹⁸ Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

¹⁹ Definition taken from Iso 31000 including modifications

²⁰ Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

Risk Identification²¹

The process of seeking out, recognising and describing **risks**

Note 1 Risk identification includes the identification of **risk sources, events**, their causes and their potential **consequences**.

Note 2 Risk identification can call upon historical data, theoretical analyses, expert opinions as well as those of other qualified persons and can take account of the requirements of **stakeholders**.

Risk Management²²

The aim of risk management is to be comprehensive and it should cover all the activities, processes and assets of the organisation. It constitutes a dynamic mechanism for the **organisation**, and is defined and implemented under its responsibility.

Risk management comprises a set of means, behaviour, procedures and actions attuned to the specific characteristics of each **organisation**, which enables General Management to keep risks at an acceptable level for the **organisation**.

Risk Management Arrangements²³

The set of means, behaviour, procedures and actions attuned to the specific characteristics of each **organisation**, which enables General Management to keep **risks** at an acceptable level for the **organisation**.

Risk Management Organisational Framework²⁴

A set of elements laying down the foundations and organisational arrangements for defining the design, implementation, monitoring, review and on-going improvement of **risk management** in the whole organisation.

Note 1 The foundations include the policy, objectives, remit and commitment in respect of **risk management**.

Note 2 The organisational arrangements include the plans, relations, responsibilities, resources, processes and activities.

Note 3 The **risk management** organisational framework is an integral part both of the strategic and operational policies, and of the whole **organisation's** practices.

Risk Management Policy

Document setting out the **organisation's** philosophy and commitment where **risk** management, taking and transfer are concerned.

Risk Management Reference Tool²⁵

The description of a framework for the implementation of a deployment process, including the essential steps to be followed. The most well-known in this area are: the AMF's* schemes for risk management and internal control, the Iso 31000 risk management standard, and COSO II.

Risk Owner²⁶

Person or entity taking responsibility for **risk** and the means for its management.

²¹ Reference : Iso 31000

²² Definition taken from the AMF* reference framework (posted on line July 22nd 2010): Risk management and internal control arrangements, and including modifications (* Autorité des Marchés Financiers, the French Financial Markets Authority)

²³ Definition taken from the White Paper "Implementation of the updated AMF reference framework" and including modifications

²⁴ Reference : Iso 31000 – the term "organisation" replaces that of "body" in the original definition

²⁵ Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

²⁶ Definition taken from Iso 31000 including modifications

Risk Register

An inventory of risks listing all the information concerning each risk of the **organisation**²⁷

Risk Source²⁸

Any element which, taken on its own or in conjunction with others, presents an intrinsic potential for creating a **risk**

Risk Tolerance

Ability of the **organisation** to accept the loss that follows the occurrence of the **risk**

Risk Treatment²⁹

Process intended to modify a **risk**

Note 1 Risk treatment can include:

- ✓ rejection of the **risk** by deciding not to start up or continue the risk-bearing activity,
- ✓ taking a **risk** or increasing it so as to grasp an opportunity,
- ✓ eliminating the **risk source**,
- ✓ modifying its likelihood,
- ✓ modifying its **consequences**,
- ✓ sharing the **risk** with one or more other parties (including contracts and **risk financing**), and
- ✓ an informed decision to keep the **risk**.

Note 2 Risk treatment measures applied to negative consequences are sometimes called "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 3 Risk treatment can give rise to new risks or modify existing risks.

Risk Universe³⁰

"Compendia of events" listing the risks (both external and internal), which are inherent to a sector of activity, to a project or to a specific area. They can list **risks**, **risk sources**, as well as observed best practices for addressing them. If their source is external, these risk catalogues must be adapted to the specific characteristics of the **organisation**; they can also be drawn up internally. In any event, they must be regularly enriched and must not constitute the sole analysis approach.

Stakeholder³¹

Person or body liable to have an impact on a decision or an activity, to be impacted or have the impression of being impacted by such decision or activity

Note : a policy-maker can be a stakeholder.

Stakeholders of the arrangements

The stakeholders of the arrangements are the board members, General Management and managers (whether they are interviewed or not)

Tools of the Risk Management Arrangements

The entire set of steering, follow-up and **risk management** tools in general: **risk cartographies**, charts, guides, presentations, yardsticks, and deliverables in general

²⁷ See p. 57 of the book "Collection Maîtrise des risques AMRAE – La cartographie: un outil de gestion des risques". P 55, for an example of the Risk register

²⁸ Definition taken from Iso 31000 including modifications

²⁹ Definition taken from Iso 31000

³⁰ Reference : "Collection Maîtrise des risques AMRAE – La cartographie : un outil de gestion des risques." P 55, see also p. 56, a chart illustrating the Risk Universe

³¹ Reference : Iso 31000

Top-Down Approach³²

An approach conducted at the highest level of the organisation relative to apprehension-causing events or a lack of opportunities that might threaten the achievement of the **organisation's** objectives. The advantage of this approach, which can be based on interviews (or workshops), is that it provides a holistic, rapid and synthetic vision of **major risks** and that it constitutes a high-level tool for sharing and harmonisation, facilitating management buy-in. This approach can be supplemented by a **Bottom-Up** approach.

Weak Signals

Perception indicators, early warning signs that may bode significant changes or events. Such weak signals can be detected via a forward-looking watch system.

³² Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"



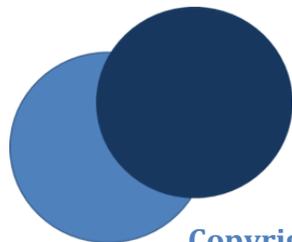
THANKS TO

AMRAE is grateful to their members for providing the major contribution to this Risk Manager framework, specially:

- Rachel Balmadier, Head of Risk, Insurance and Internal Control, Compagnie des Alpes
- Laurent Barbagli, Head of Risk and Insurance, Lafarge- Amrae's board member
- Brigitte Bouquot, Head of Insurance and Risk management, Thalès - Amrae's board member
- Bruno Dunoyer de Segonzac, Risk Management & Internal control Consultant coach
- Françoise Gaucher, Risk Management Expert, Groupe La Poste
- Bénédicte Huot de Luze, Chief Executive, AMRAE
- Gérard Lancner, President Advisor AMRAE
- François Malan, Head of Risk, Nexity - Amrae's board member - **Group Chair**
- Anne Piot d'Abzac, Head of Compliance and Risk, Ipsen Pharma
- Sylvie Pugnet, Lawyer
- Philippe Viénot, Risk Manager, BNP Paribas- Amrae's board member



www.amrae.fr



Copyright ©AMRAE 2013

This framework, owned by AMRAE, is protected by copyright.
Any quote or reproduction, in whole or in part, shall be allowed
subject to the copyright mention ©AMRAE 2013.