Risk Manager

Tasks & Competencies

AMRAE
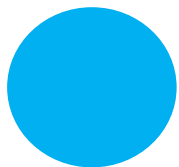
Foreword

Risk management professionals are thriving and growing in our organisations, in France and around the world. However the profession is also undergoing tremendous changes.

To heighten the visibility of the risk-managers' profession, their level of technical skills and their added value, it has become necessary to develop a Risk Manager's core competencies set – a true framework to understand the activities and tasks undertaken, and skills needed by the risk-manager.

AMRAE is proud to introduce the *first* **Risk Manager's Core Competencies** set. It is the result of the combined insight gained by ten years of professional development offered through the AMRAE, our biennial surveys of risk-management professionals, and our members' formal and informal interaction about their respective experiences.

With this document, we provide an outline for a risk manager's job description, including its tasks and competencies and its contribution to the organisation. Fundamentally, risk managers work alongside top management to assist them in identifying critical risks and their optimal treatment.
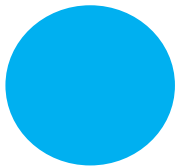
With this report we offer those responsible for further education a set of competencies required for the successful training today's risk managers. This document is also our contribution to the ongoing dialogue on the future of our profession with our European colleagues and with the worldwide RM community. As the profession will evolve we are committed to updating and maintaining this competency set as changes in business requirements evolve.

Our warmest thanks go to the working group chaired by François Malan, the risk manager of Nexity, for their contribution in achieving such an accomplishment.

We remain strongly committed to providing added value to all our member organisations.

Gilbert Canaméras

Chairman AMRAE

4

Contents

Presentation of the AMRAE Missions & Competencies set

Since 2010, the AMRAE has been working to define the Risk Manager's professional core competencies set.

FERMA, for its part, has embarked in a campaign to promote the recognition of the profession.. Towards this end, they have launched a competencies accreditation project, which will be based on a set of competencies needed by the efficient risk manager (and not to assess the efficiency of the Risk Management).

As it is a Risk Managers' professional association, and in complement to the efforts of FERMA, AMRAE has researched and developed a vision of the profession, listing the tasks, and the skills and competencies required for a person to become successful in Risk-Management.

AMRAE has a unique blend of specific talents and tools that are essential for building a cohesive vision and competency set for the profession:

- For over 10 years, "AMRAE Formation" has developed and offered education seminars dealing with the Risk Manager's mission and the skills and competencies needed for a person to be considered a risk management professional.

- Three editions of the Risk Manager Barometer (2009-2011-2013) have gathered important information on the missions, profile, compensation and future of the profession.

- AMRAE members' feedback session, experience sharing, and forum of discussion provide up-to-date understanding of the prerequisites, competencies and skills essential to their profession.

Caveat

AMRAE's intention in developing this competencies set is to offer the broadest overview possible for a Risk-Manager's missions and tasks. There will be some risk managers who, because of unique circumstances or needs in their organization require competencies that are not included on the list. Therefore this competency set should be considered a core set from which additional competencies, when required, can be added. There will be some who work in risk management in very narrow and specialized segments such as insurance purchasing or loss control which require only a few of the competencies. However, for even the specialist, understanding risk management means being familiar and reasonably conversant with all of the core competencies of risk management.

AMRAE's project is not limited to a one-time effort. We are committed to work together to modify and extend the competency set as emerging needs of business, industry, and government are identified. . .
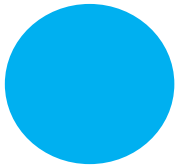
Risk Management

Definition[1]

Risk management concerns all the internal and external stakeholders in an organisation. It should be global and integrated and cover all the activities, processes and assets of the organisation.

Risk management is a dynamic system within the organisation, developed and implemented under the responsibility of the organization's leadership at all levels.

Risk management consists in a set of resources, behaviours, procedures and actions tailored to suit the characteristics of the organisation, permitting top management to identify and manage risks they choose to accept at levels deemed tolerable by the organisation's leadership and which can directly or indirectly affect adversely or positively the strategy of the enterprise.

Risk is defined here as the possibility of an event occurring, the existence of which is likely to generate losses or opportunities to staff, assets, environment and objectives of the organisation or to its reputation.

Risk management objectives:

- To create or preserve value, assets, and reputation of the organisation.
- To secure decision-making and other processes in the organisation to improve the odds of it achieving its objectives
- To improve coherence between the organisation's actions and values
- To improve staff support for a shared vision of the major risks.
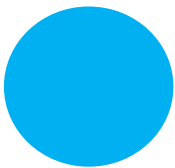
The Risk Manager

Depending on the organisation, the Risk Manager may be in charge of all or part Risk management activities, which include the following :

- Definition of the risk management missions, framework, and process
- Risk Assessment (risk identification, analysis, evaluation)
- Risk control (to an acceptable level, function of the chosen risk criteria)
- Ensure that all staff embrace risk culture
- Risk financing aligned with the risk management policy
- Managing the aftermath of uninsured as well as uninsurable events
- Claims Management
- Business Continuity Management
- Crisis management
- Monitoring and Reporting

The risk manager presents to Top Management the organisation's risk profile and optimised reduction and finance solutions, within the limits of the risk appetite and risk tolerance defined by the organisation's board of directors or board of governors.

---

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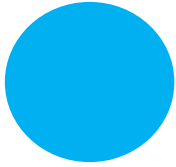
Organisation

The risk-manager should be able to:

- Define his duties clearly, to perform efficiently
- Developing clear and precise action plan and objectives
- Prioritising and planning of actions
- Monitor the execution of tasks delegated to others

Management

The risk-manager should be able to:

- Organise and support teamwork
- Provide specific instructions, and a clear vision
- Enhance support by all stakeholders: Top Management, departments' heads, teams, projects' managers, contacts at operational level
- Build trust and confidence to enhance support of shared objectives

Curiosity and Scepticism

The risk-manager should be able to:

- Listen carefully when conversing with internal and external stakeholders
- Detect weak signals
Ask questions and challenge assumptions, remain objective, and keep an open and unprejudiced mind

Communication

The risk-manager should be able to:

- Behave and speak appropriately, and encourage dialogue and trust
- Write and speak in a clear and convincing manner
Develop communication strategies that meet organizational needs and style

- Embody leadership
- Understand the argument of the other party in a negotiation, and bargaining with diplomacy
- Promote transparency in information, while understanding the need for confidentiality
- Negotiate with the best interests of the organisation in mind

Creativity and Adaptability

The risk-manager should be able to:

- Change the course of actions when made necessary by a changing context
- Address each party in a way that can be easily understood
- Engineer the changes needed in the organisation to improve its performance and keep it aligned with its overall objectives while taking into account external constraints, and particularly the evolution in regulations.
- Think the unthinkable; challenge the established 'truths'
- Propose new approaches and visions
- Develop innovative frameworks and tools

Culture and awareness of what is at stake

The risk-manager should be able to:

- Develop a sound understanding of macro issues (economic, financial…), and the environment (competition…)
- Understand what is at stake, the different trades and markets in which the organisation operates
- Develop insight into the culture and environment of the countries where the company is operating currently and those in which it contemplates future operations
- Adhere to the organisation's values, and act accordingly

Manage Stress: Stress Reduction

The risk-manager should be able to:

- Analyse a situation with an objective mind, make effective decisions, event in the event of situations of extreme emergency
- Accept critics and question his/her own judgment

ACTIVITY

Definition of the missions and structure of the RM framework

1

TASKS
• Define the missions entrusted to the risk manager in the context of organizational strategy
• Assess threats and opportunities generated by the strategy
• Identify activities, processes (businesses services) that are part of organizational strategy
• Develop and implement the risk management framework that will be necessary to manage critical risks to strategy
• Develop an appropriate risk management methodology & reference table of the common lexicon of risk terms that the organization has agreed to
• Develop risk management policy, taking into account the risk appetite and tolerance defined by top management and/or of the organisation's governance authorities.
• Secure approval by top management and/or the Organisation's Governance Authorities   of the risk management policy frameworks, as well as the allocation of the resources needed for their implementation

REQUIREMENTS	QUALITY/SKILLS
Taking into account the culture, history and specificity of the organisation and its context (competition...):	• Organisation
Define objectives for the risk management plan and demonstrate their benefits	• Curiosity and Scepticism
Secure approval of these objectives by the organisation's governance authorities and ensure that they are known by everyone (all stakeholders involved in the risk management effort)	
When needed, make present arguments or reports to the authorities in charge of strategic planning	• Culture and awareness of what is at stakes
Provide methodological approaches for the identification, analysis and evaluation of risks involved in new strategic directions or initiatives	• Creativity and Adaptability
Understand the stakes, constraints, and objectives specific to different activities, s	• Organisation
Understand the organisation's structure and role and value of the different activities within the organisation	
Identify of the roles and responsibilities of all organisation's staff	
Define a target organisational structure to enhance the organisation's overall performance.	• Organisation
Build a department and framework that is consistent with the company's strategy and risk attitude and tolerance; communicate to those involved (Top management & other managers, operational pilots...)	• Creativity and Adaptability
Define the needed resources: e.g. human resources, IT, Finance, other	• Culture and awareness of what is at stakes
Set up one (or more) risk committee(s)	
Define interactions with internal audit and internal control	
Develop the reporting structure to fulfil stakeholders' expectations	
Select a Risk Management framework and, if necessary, adapt it as required by the specificity of the organisation	• Organisation
Define the implementation plan	
Identify and confirm in writing the strategic objectives of the organization and from this derive, write, and confirm the operational objectives required to achieve the strategy.	• Curiosity and Scepticism
Develop the mission, the objectives and the scope (including the various activities) of the risk management policy and align this with company strategy	• Culture and awareness of what is at stakes
Define the principles underlying the risk mitigation policy of the organisation (acceptance, avoidance, reduction, separation/segregation and transfer)	• Communication
Define and implement the risk-financing strategy (retention, transfer....)	
Define the acceptable limits of risk for the organisation (risk tolerance).	
Secure top management's approval of the four preceding components: mission objective and scope, risk mitigation, risk financing, and risk tolerance	
Then write-up these components in a risk management policy document to be communicated to those concerned (Board Members, Top management, etc.)	
Compile and explain the missions, structures and resources to the operational managers	• Management
Make the point of the value created through the missions, structures and resources of risk-management	•
	• Communication

TASKS

ACTIVITY

Risk assessment (Risk identification, analysis and evaluation)

2

- Select the tools needed for risk assessment (scales, interview guide, risk register, risk universe, risk lexicon…)
- Anticipate risks and follow-up all risks evolution (in coordination with economic and business intelligence)
- Lead individual interviews with top management and other managers to identify critical risks
- Facilitate risk identification, analysis and evaluation (prioritization) workshops at all levels of the organization including risk identification for new projects and processes
- Map risks by unit/business segment or by major project
- Identify the organisation's most critical risks and ensure top management concur with the list.

REQUIREMENTS	QUALITIES / SKILLS
Develop a risk universe for the organisation	• Organisation
Develop a specific scale to quantify the potential impact should the risk occur and develop another scale for risk frequency. Then combine both scales into a tool for management to assess the frequency and impact in terms that relate to strategy	• Creativity and Adaptability
With key decision-makers define and implement a glossary, spread it throughout the organisation	• Curiosity, Scepticism, and Ability to listen
Explain, when necessary the difference between gross and residual risks	
Select the appropriate format for the risk register	
Develop a risk interview guide and communicate it to those concerned	
Define the specific reporting formats and frequencies for the risk management activities	
Select the tools needed for stakeholders' risk assessment.	
Communicate with Internal Audit on risk management issues and processes	
Establish the inventory of the processes for all organisation's activities for strategic, business and regulatory intelligence	• Curiosity, Scepticism, and Ability to listen
Provide input for strategic intelligence through the carefully selected formation gathered during the missions	• Organisation
Analyse weak signals involving risk, attitude, and treatment	
Include relevant weak signals in the risk assessment process	
Identify critical risks, their causes and their potential impact	• Stress Reduction
Enable and encourage methods for the identification and disclosure of both opportunities and threats	• Susceptibility
Quantify risks both gross and residual	
Clarify, summarise and rephrase the discussions that have taken place during the risk assessment process using the common risk lexicon	• Communication
Use and update the risk management framework	
Act as leader or moderator for a group of top management, other managers and, when needed, engage the services of experts	• Communication
Encourage the identification of opportunities as well as threats	• Susceptibility
Identify risks, their causes and their potential impact	
Analyse risks, both gross and residual	• Stress Reduction
Clarify, summarise and rephrase the discussions that have taken place during the risk assessment process	
Establish a risk matrix aligned with the organisation's needs and those of each entity/business unit, or of the project concerned	• Organisation
Update & keep a record the history of risk maps	• Management
Organise risk feedback sessions and experience sharing from all the entities concerned	
Challenge the risks identified in the various entities – Analyse potential correlation	• Organisation and Curiosity and Scepticism
Consolidate retained risks	• Management
Develop the consolidated risk map for the stakeholders	

TASKS

ACTIVITY

Risk control *(to an acceptable level, dictated by the chosen risk criteria)*

3

- Present / Validate the most critical risks
- Identify the full range of available risk treatment tools
- Participate in drafting action plans
- Analyse and implement risk treatment action plans
- Assist during mergers & acquisitions due diligence process
- Visit hazardous units and other places where risk is critical
- Consolidate, monitor and review action plans

REQUIREMENTS	QUALITIES / SKILLS
Summarise risks deemed critical for the attention of top management Secure validation of priorities in dealing with the critical risks Secure the appointment of a risk owner for each of the critical risks	• Organisation • Curiosity and Scepticism
List all operational methods of dealing with specific risks (construction, training…) List all risk financing programmes (insurance covers, captives and others, including retention and reserving) List all internal control activities List Business Continuity Plans and ensure they are regularly exercised List all crisis management plans and ensure they are regularly exercised Define the criteria against which the aforementioned risk treatment tools efficiency is assessed	• Organisation • Management
Suggest further risk treatment solutions in addition to those of the risk owners Participate in the developing business continuity plans Participate in the development risk prevention plans Develop risk assessment, with the assistance of specialists (internal, and where needed, external experts) and follow up insurers' recommendations Carry out training and other risk awareness raising activities (road safety, expats, new employees…) Secure validation of risk treatment by other "support" functions concerned Define jointly with each risk owner, a timetable for the implementation of the action plan	• Culture and awareness of what is at stakes • Creativity and Adaptability • Organisation • Management
Identify risk areas Develop risk treatment plans taking into account the criticality of the risk areas and the organisation's risk appetite	• Susceptibility • Creativity
Highlight the risks that may potentially jeopardize proposed mergers & acquisitions Identify and evaluate post-mergers & acquisitions risks Suggest appropriate risk treatment measures Align insurance or retention coverage with the future operation after merger	• Susceptibility • Creativity • Management
Hire specialists to assist in the process (internal and, where needed, external experts) Advise with respect to the obvious immediate operational actions required to mitigate or treat risks Organise regular meetings with risk correspondents in operational units or those in charge of risk areas	• Communication
Draw up actions and budgets, risk by risk Support the implementation of risk treatment measures decided by the risk owner Develop the consolidated action plans for the stakeholders	• Organisation • Communication • Stress reduction

TASKS

ACTIVITY

Dissemination of risk culture

4

- Develop, lead, and train a network of risk correspondents in operational units
- Participate in important events (seminars, committees…)
- Draft internal communication concerning risk culture

REQUIREMENTS	QUALITIES / SKILLS
Spread risk culture in line with the defined policy	• Communication
Train correspondents so that they understand the methodology, their role and the risk management operations	
Organise sharing of best practices and feedback sessions and experience sharing among risk correspondents in operational units in operational units	• Management
Participate and, where needed, play a role in these events and communicate on risk culture, on measures for dealing with the critical risks …	• Communication
Encourage feedback sessions and experience sharing on event and incident	
Using a few simple explanations, clarify the components of risk culture (actions carried out, feedback sessions and experience sharing, implementation timetable…)	• Communication
Spread this communication using various internal channels	• Management
Spread risk culture in line with the defined policy	
Train risk correspondents in operational units so that they understand the methodology, their role and the risk management operations	

TASKS

ACTIVITY

Risk financing

in line with the finance strategy

5

- List all risk-financing options
- Organise relations with service providers (brokers or agent, insurers)
- Negotiate insurance contracts
- Administer and deploy insurance coverage
- Set-up and manage a captive

REQUIREMENTS	QUALITIES / SKILLS
Look for available solutions fulfilling the organisation's needs (Insurance, retention or alternative systems, including the different types of captive schemes available on the market)	• Culture and awareness of what is at stakes
Monitor and benchmark the risk-financing solutions offered by the markets (insurance companies, banks, financial markets)	• Creativity Adaptability
Define the resources associated with these solutions, develop cost/benefit analysis	• Organisation
Develop criteria for the selection of service providers	
Secure validation of the various components of risk financing mechanisms: model, resources, selection criteria	
Identify potential service providers	• Organisation
Define terms and conditions for each service-provider, in line with professional rules and practices, with specific to the roles of each party and their remuneration level and structure	• Communication
Define performance criteria	
Negotiate and formalise the service contract with the broker	
Analyse the insurance proposal (wording, limits, excesses…) in line with the organisation's identified needs (insured sums and cover) / define endorsement forms	• Stress Reduction
Define the main contractual clauses and performance criteria	• Susceptibility Ability to listen
Monitor the insurance contracts drafting / validating by the broker	
Spread throughout the organisation information concerning the covers (contents, exclusions…)	• Organisation
Monitor premium payments, contract renewals, and any renegotiation	• Management
Monitor performance criteria	• Communication
Consolidate annual results (claims experience, policy costs, shortcomings, cover…) and report to internal decision-makers and the different stakeholders (both internal and external)	
Adapt cover to the evolution of risks and to required insured sums	
Analyse the benefits, the objectives and the feasibility of a "captive scheme"	• Culture and awareness of what is at stakes
Select the partners (actuary, manager…) and organise the implementation of the "captive" if a captive's formation is warranted	• Organisation
Participate in the management of the "captive"	
Comply with all regulations and communication requirements associated with the "captive"	

TASKS

ACTIVITY

Handling uninsured / uninsurable events

6

- Carefully describe the potential event
- Identify and assess resources and action plans
- Monitor feedback sessions and experience sharing

REQUIREMENTS	QUALITIES / SKILLS
Define the scope, the stakes, the consequences…	• Organisation
Collect information from stakeholders	• Curiosity, Scepticism, and Ability to listen
Where appropriate, define the resources and implement action plans	• Organisation
Verify that resources and action plans are consistent with expectations	• Stress Reduction
List occurrences of similar events within the organisation	• Curiosity, Scepticism, and Ability to Listen
Identify triggers	• Communication
Where appropriate, inform the Governance authorities	
Where appropriate, update risk maps and/or action plans	

ACTIVITY

Claims handling

7

TASKS

- Characterizing events in order to determine applicable coverage and potential liability, if any
- Organizing claims management with partners (brokers or agents, insurers, loss adjusters, even reinsurers…)
- Following-up compensation processes
- Validation of back to normal activities status

REQUIREMENTS	QUALITIES / SKILLS
Collect information concerning risk events	• Communication
Provide the information collected to the governance authorities to feed internal and/or external communication	• Organisation
Check whether an insurance contract can provide a compensation or whether a self insurance mechanism is involved in the claim's handling process (in that case have proper loss reserving set up)	• Management
Trigger the crisis response, business continuity and business resumption procedures (or verify that they have been triggered)	• Stress Reduction
Verify with the risk owner the nature and impact of each events	
Analyse the causes of the loss and its financial and reputational impact, check the quality of the data provided.	
Examine whether third parties could be liable thus opening the possibility of a recourse	
Put in the claim or check the compliance of the claim submission with all contract obligations (conditions and claim form)	• Organisation
Organise negotiations with partners concerning the event description, the quantum of loss, the conditions applicable to the indemnity owned, the insurance program administration process including loss reserves set-up by insurers.	• Stress Reduction
Define the administrative process and corrective measures	• Management
Identify the loss adjusters' missions, negotiate the conditions for the compensation process (timing, cost) and put in place regular monitoring.	
Monitor the claims handling plan, using regular reporting from the interested parties, both internal and external (service providers)	• Organisation
Validate the claim settlement	• Management
Keep Top Management informed and ensure that internal and external communication is both relevant (in accordance with the organisation's strategy) and updated regularly.	• Communication
Check with partners and key internal actors that the activity is back to normal (nominal)	• Organisation
Evaluate the performance of partners against the performance criteria and expected results	• Communication
Develop corrective actions to prevent the occurrence of a similar event (define desirable improvements concerning insurance covers and sums insured)	
Organise feedback sessions & experience sharing	

TASKS

ACTIVITY

Monitor & Review

9

- Maintain & continuously improve   the risk management plans
- Facilitate the risk committee
- Report to the risk management plans' stakeholders
- Effectively communicate to external stakeholders
- Develop effective relations with internal audit

REQUIREMENTS	QUALITIES / SKILLS
Drive the risk management plans implementation	• Culture and awareness of what is at stakes
Develop and implement risk-monitoring dashboards, and assess the risk management activities and their performance	• Creativity and adaptability
Define and implement risk-monitoring and e risk management plans implementation indicators	• Organisation
Identify the risk committee(s)members: define the role and operating procedures of the risk committee(s)	• Communication
Facilitate the committee(s), prepare the agenda and anticipate arbitrations	• Curiosity, Scepticism and the Ability to Listen
Define with stakeholders the risk management plan's format and operating procedures	• Communication
Explain to stakeholders the risk management plan's deliverables (mapping, monitor & review plans, analyses, indicators…)	• Stress Reduction
Explain information on the organisation's risks to those in charge of financial communication	• Communication
Execution of deliverables for supervisory authorities, drafting the "risk factors" section in the reference document	• Organisation
Participate in developing the audit plan	• Curiosity, Scepticism and the Ability to Listen
Collect information for risk management purposes (new risks, evaluation…)	

ACTIVITY

Steering and Reporting

9

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

REQUIREMENTS	QUALITIES / SKILLS
Act as the driving force behind the arrangements	• Culture and awareness of what is at stakes
Establish and disseminate risk-monitoring dashboards, together with an assessment of the risk management activities and their efficacy	• Creativity and adaptability
Define and apply risk-monitoring indicators and those for the implementation of the risk management arrangements	• Organisation
Identify participants in the risk committee(s): define the role and operating procedures of the risk committee(s)	• Communication
Facilitate the committee(s), prepare the agenda and plan forward for arbitrations	• Curiosity, Scepticism and the Ability to Listen
Define with stakeholders the arrangements' format and operating procedures	• Communication
Present to stakeholders the arrangements' deliverables (cartography, follow-up of action plans, analyses, indicators…)	• Stress Reduction
Present information on the organisation's risks to those in charge of financial communication	• Communication
Execution of deliverables for supervisory authorities, drafting the "risk factors" section in the reference document	• Organisation
Participate in drawing up the audit plan	• Curiosity, Scepticism and the Ability to Listen
Gather information useful for risk management (new risks, evaluation…)	
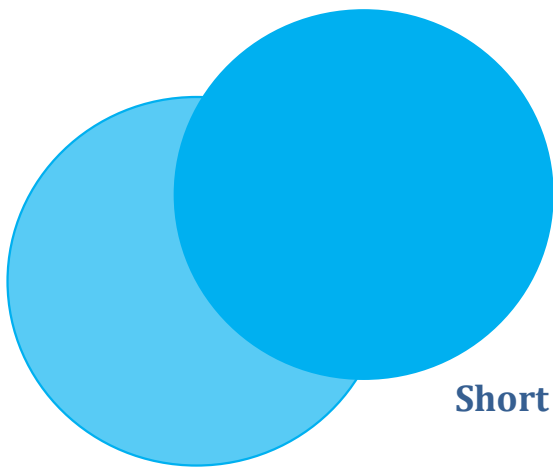
APPENDIX

Short Risk Management Glossary

AMRAE Risk Manager Missions and Competencies

Bottom-Up Approach[2]

Process for the **identification** and **evaluation of threats or lack of opportunities** within entities, Business Units, areas… that could derail the organisation's objectives, consolidated at corporate level. This process can be based on existing risk management processes, such as the analysis of regulatory risks, and further enriched by an analysis of operational risks. This process enables the involvement of the various operational levels and their associated risks, with which top management is often not familiar enough, and facilitates the implementation of efficient action plans so as to comfort the results. This process can be carried out in addition to the **Top-Down approach**.

Captive[3]

- ✓ 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 purpose is to provide insurance cover concerning exclusively the **risks** of organisation or organisations who own it or alternatively the **risks** of one or more other companies belonging to its economic family..

- ✓ 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 purpose is to provide reinsurance covers concerning exclusively the **risks** of the organisation or organisations who own it or alternatively the **risks** of one or more other companies belonging to its economic family.

Consequence[4]

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/unit

Department or subsidiary of the **Organisation**

External Context[5]

External environment within which the organisation seeks to attain its objectives

Note: The external context can comprise:

---

[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 – ISO Guide 73
[5] Definition taken from ISO 31000 including modifications

- ✓ 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

Top Management, Board of Directors or Supervisory Board, Meetings of elected representatives,

Internal Audit[6]

An independent and objective function providing the **organisation** assurance with respect to 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 Context[7]

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

Note: The internal context can comprise:
- ✓ the governance, the organisational structure, roles and accountabilities,
- ✓ 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 Control[8]

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 critical risks, whether they be operational, financial or those of compliance.

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

- ✓ compliance with laws and regulations;
- ✓ proper implementation of the instructions and guidelines laid down by Top Management or the Board;

---

[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)

- ✓ correct functioning of the organisation's internal processes, in particular those contributing to the conservation of its assets;
- ✓ reliability of its financial information

Interview guide

A list of question that risk management practitioners should ask risk owners to help identify, analyse, evaluate risks in a consistent manner throughout the organisations

Level of risk[9]

Magnitude of a **risk** expressed in terms of the combination of **consequences** and their **likelihood[10]**
Outcome of a risk analysis or evaluation (taking into account its criticality and its control). The result can be broken down into the level of **gross risk** *(analysis),* level of **residual risk** *(evaluation)* and level of target residual risk.

Critical Risk

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

Monitoring[11]

Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

Note: Monitoring can be applied to a **risk management framework**, **risk management process**, **risk,** or **control**
Checking, supervision, critical observation or assessment of the status with a view to continual

Organisation

The organisation is the company or public organisation concerned

Gross Risk[12]

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

Residual Risk[13]

Risk remaining after risk treatment
A residual risk may include an unidentified risk.

The residual risk can also be called "net risk"

Risk

Effect of uncertainty on objectives

Note 1: An effect is a deviation from the expected — positive and/or negative.
Note 2: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
Note 3:: Risk is often characterized by reference to potential **events** and **consequences**, or a combination of these.
Note 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** of occurrence.
Note 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood

---

[9] Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"
[10] Reference : Iso 31000 - Guide ISO 73
[11] Reference : Iso 31000
[12] Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management" including modifications
[13] Definition taken from Iso 31000 including modifications

Risk Analysis[14]

A process put in place 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.

Risk Appetite[15]

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

Risk Areas

Specific risk domain defined within the organisation. Often referred to as key risk areas when limited to critical risk having a direct impact on the achievement of the organisation's goals and objectives

Risk Assessment[16]

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

Risk Map [17]

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.

Note 1 – Professional also define risk matrix[18] - tool for ranking and displaying **risks** by defining ranges for **consequence** and **likelihood**

Risk Committee

Depending on the organisation, a committee comprising, , 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 Correspondents[19]

Members of the risk management internal network responsible for following risk management activities at the local level within each entity, and under the authority of the Risk Manager, and for being the instrumental in the implementation of the **risk management** process

They participate in the **risk mapping exercise**, inform the Risk Manager of the occurrence of critical new **risks** and assist **risk owners** in the preparation of action plans.

Risk Criteria[20]

Terms of reference against which the significance of a **risk** is evaluated. Risk criteria can include risks and benefits, legal and regulatory requirements, social, economic and environmental dimensions, **stakeholders'** concerns, priorities and other assessment criteria.

Note 1: Risk criteria are based on organizational objectives, and **external** and **internal context**
Note 2: Risk criteria can be derived from standards laws, policies and other requirements.

---

[14] Reference : Iso 31000
[15] Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"
[16] Reference : Iso 31000
[17] Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"
[18] Reference : Iso 31000 - ISO Guide 73
[19] Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"
[20] Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

Risk Culture

The system of values and behaviours present throughout an organization that shape risk decisions. Risk culture influences the decisions of management and employees, even if they are not consciously weighing risks and benefits. It should identify cultural strengths as well as opportunities for improvement with regard to risk management.

Risk Evaluation[21]

Process of comparing the results of **risk analysis** with **risk criteria** (3.3.1.3) to determine whether the **risk** and/or its magnitude is acceptable or tolerable

Note: Risk evaluation assists in the decision about **risk treatment**

Risk Financing[22]

Form of **risk treatment i**nvolving contingent arrangements for the provision of funds to meet or modify the financial **consequences** should they occur.

Note 1: Mechanism, the aim of which is to have all or part of the risk borne by an outside third party (insurance, captive…).
Note 2: The term can also designate provisions intended to cover the costs of implementing risk treatment.

Risk Identification[23]

The process of finding, recognizing 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 Management[24]

Coordinated activities to direct and control an organization with regard to **risk.**
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 Framework[25]

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 Framework[26]

A set of components 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.

---

[21] Definition taken from Iso 31000 including modifications
[22] Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"
[23] Reference : Iso 31000
[24] 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)
[25] Definition taken from the White Paper "Implementation of the updated AMF reference framework" and including modifications
[26] Reference : Iso 31000 – the term "organisation" replaces that of "body" in the original definition

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

Statement of the overall intentions and direction of an organization related to **risk management.** Document setting out the **organisation**'s philosophy and commitment where **risk** management, including risk treatment, are concerned.

Risk Management Reference Tool[27]

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 Map

The risk map is based on an analysis of business processes, which is crossed with the typology of risks. For each event, risk is assessed in terms of:
- Probability of occurrence,
- Resulting loss in case of realisation.

Each event with possible risk must be assigned to a risk category, to the business line where the incident would occur. The maps should include the identification of key risk indicators: these are quantifiable elements that may increase the likelihood of the occurrence of a risk such as number of transactions processed, absenteeism rate, etc.

Risk Matrix

A two-dimensional array to visualise the two traditional dimensions of risk (likelihood and impact) in order to display the ranking of a risk and see the risk ranking class it belongs to. The number of columns and rows in a risk matrix can be different depending on how much refined the risk assessment shall be. The likelihood could range from 'very unlikely' and 'unlikely', via 'occasional' to 'likely' and 'very likely'. Consequences of a risk could range from 'negligible' and 'minor' via 'moderate' to 'major' and 'extreme'.

Risk Owner[28]

Person or entity with the accountability and authority to manage the **risk**.

Risk Register

Record of information about identified **risks.** An inventory of risks listing all the information concerning each risk of the **organisation**[29]

Note: The term "risk log" is sometimes used instead of "risk register".

Risk Source[30]

Element which alone or in combination has the intrinsic potential to give rise to **risk**
Note: A risk source can be tangible or intangible

Risk Tolerance *(see also Risk Appetite)*

Organisation's or **stakeholder**s' readiness to bear the **risk** after **risk treatment** in order to achieve its objectives. Also Ability of the **organisation** to accept the loss that follows the occurrence of the **risk**

Note: Risk tolerance can be influenced by legal or regulatory requirements.

---

[27] Reference : "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"
[28] Definition taken from Iso 31000 - ISO Guide 73
[29] 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
[30] Definition taken from Iso 31000 including modifications

Risk Treatment[31]
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 Universe[32]
"Compendia of events" listing the risks (both from external and internal sources), 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.

Stakeholder[33]
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.

Note1: ISO recommend now the alternative "interested party"
Note 2: a policy-maker can be a stakeholder.

Stakeholders of the risk management efforts
The stakeholders of the risk management efforts are the board members (directors), Top Management and managers (all operational managers whether they are interviewed or not)

Tools of the Risk Management Efforts
The entire set of monitoring and review and other **risk management** tools: **risk mapping**, matrix, charts, guides, presentations, yardsticks, and deliverables

Top-Down Approach[34]
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 **critical 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.

---

[31] Definition taken from Iso 31000
[32] 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
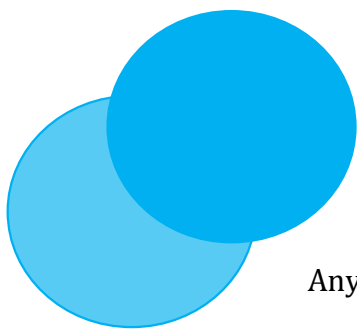[33] Reference : Iso 31000 – Guide ISO 73
[34] Definition taking its inspiration from the book: "Collection Maîtrise des risques AMRAE – Trajectoire vers un Enterprise Risk Management"

THANKS TO

- François Malan, Head of Risk, Nexity – Group Chair
- Laurent Barbagli, Head of Risk and Insurance, Lafarge
- Françoise Gaucher, Risk Management Expert, Groupe La Poste
- Anne Piot d'Abzac, Head of Compliance and Risk, Ipsen
- Bruno Dunoyer de Segonzac, Risk Management Consultant
- Rachel Balmadier, Head of Risk, Insurance and Internal Control, Compagnie des Alpes
- Philippe Viénot, Risk Manager BNP Paribas
- Sylvie Pugnet, Lawyer
- Bénédicte Huot de Luze, Chief Executive Officer, AMRAE