Extended Partnership

multi-Risk sciEnce for resilienT commUnities undeR a changiNg climate

Spoke 7 – TS3 – Communities' resilience to risks: social, economic, legal and cultural dimensions
WP 7.7 – Legal and Ethical Aspects Prospect
Task 7.7.5 – Profiles of responsibility, compliance, and accountability of the Civil Protection System

DV 7.7.10

Methodology for assessing the legal risk of decision-makers

Analysis of responsibility profiles and mapping of risk processes: the "Audit" of Fondazione CIMA

Document versions:

Authors	**Actions**	**Date**
Francesca Munerol (CIMA)	Drafting	May 1st
Marco Altamura (CIMA) Luca Molini (CIMA)	Intermediate revision	August 3rd
Marina Morando (CIMA)	Final revision	September 25th

Table of Contents

Introduction

As part of the RETURN project (multi-Risk sciEnce for resilient communities under a changing climate), **Spoke 7 – TS3: Communities' resilience to risks: social, economic, legal, and cultural dimensions** aims to promote a correct perception of risk at all levels—considering psychological and educational aspects—and to incorporate risk uncertainty into cognitive and decision-making processes. To this end, support is provided in preparing and building the resilience of the population exposed to risks through specific information, education, training, and participation processes, and in the definition of technological, methodological, and political risk mitigation measures for the protection of cultural and natural heritage. Among the dimensions explored by this Spoke is research on liability profiles in decision-making chains: **WP 7.7 – Legal and Ethical Aspects Prospect** intends to conduct a critical assessment of the multilevel institutional and legislative frameworks relevant to environmental risks, in relation to the ethical dimension of risk, identifying gaps/conflicts, overlaps, and inconsistencies. The specific objective is to propose some remedies, after conducting a review of liability and accountability profiles with reference to national and international contexts, promoting the transition from "law of liability for natural risks" to "prevention of such risks." It follows that **Task 7.7.5 – Profiles of responsibility, compliance, and accountability of the Civil Protection System** , for which the CIMA Foundation is responsible, aims to strengthen awareness of the legal responsibility of and in the Operators of the National Civil Protection System, with a view to the efficiency and effectiveness of the system, good governance, certainty and adequacy of the regulatory framework, as well as the dissemination of the culture of PC.

CIMA Foundation Activities

Before reporting on the outcome of the part of the Project carried out by the CIMA Foundation on the aforementioned Task, it seems appropriate to acknowledge what it normally carries out within the research programme called *Governance & Responsibility in Civil Protection Systems:*

(I) Analysis and study of relevant case law regarding legal cases - both national and international, where significant - involving Civil Protection or, more generally, PC risks, for an examination of the critical issues of prediction, evaluation and decision-making procedures, the critical issues of technological tools, which have emerged following *ex post judicial review* and litigation in general.

(II) systematization of case studies in WikiProcessi (https://wikiprocessi.cimafoundation.org) , a platform owned by the Department of Civil Protection, created and managed by the CIMA Foundation as the Department's centre of expertise on the subject of liability in civil protection;

(III) advanced training on the legal responsibility of Service Operators National Civil Protection.

(IV) support the Department in disseminating issues regarding responsibility for protection activities;

(V) support in identifying the "regulatory needs" for the System, in the formation and analysis of the regulations and procedures applied, for the optimal functioning of the SNPC and the Observatory of good civil protection practices;

(VI) Auditing activities of the complex structures of the SNPC – such as Functional Centers and Operations Rooms – to ensure greater compliance.

In relation to this last point, this work intends—in the context of the Project—to systematize this activity and, on the other, to provide an updated, or "state-of-the-art", representation. This will, on the one hand, place this activity within the framework of the most innovative *internal audits* , and, on the other, initiate a sharing and critical comparison of the methodology and results with a wider audience than has been previously involved.

To grasp the effort of this work, it is worth pointing out from now that:

- the auditing activity concerned the bodies responsible for regional and national forecasting, monitoring and warning functions with regards to natural risks and

in particular hydrogeological and hydraulic ones and aimed at verifying compliance with the regulatory framework, as well as the existence, quality and observance of the procedures and operating practices adopted by the Body itself, also in comparison with the "best practices" operating at other centres of equal rank.

- The audit was structured into a series of interrelated and successive phases – which will be discussed in greater detail later – aimed at analyzing, examining, and clarifying the legal responsibilities of operators at various levels who are responsible for forecasting, monitoring/surveillance, and communicating critical issues triggered by natural and manmade risks, within the context of the National Civil Protection Service's early warning system.

- the analysis activities conclude with the definition – in terms that are as objective and scientific as possible – of the audited entity's exposure to legal and reputational risk.

- Close collaboration between the auditor and the organization itself has always been expected: while the auditor pools its multidisciplinary *expertise*, the organization undergoing the assessment is required not only to share all data, documents, procedures, and practices necessary to conduct the in-depth analysis, but also to actively involve the personnel assigned or otherwise involved in the processes. This has led to the need to schedule regular group and individual meetings and interviews to thoroughly investigate all issues necessary for carrying out the activities. Specifically, the critical analysis of the organization's direct processes, with specific reference to the organizational structure and functioning of the entire structure, is based on a systemic approach, resulting in increased knowledge and awareness of the legal responsibilities associated with civil protection activities.

- The systemic approach required that, in addition to the internal processes of the audited entity, stakeholders in the entity's activities be involved – wherever possible – that is, all those branches of the regional civil protection system that provide or receive products or services to or from the entity itself.

Below, therefore, is the result of the systematization and representation of this activity, as actually carried out by the CIMA Foundation at institutions responsible for forecasting, monitoring/surveillance, and communicating critical situations triggered by natural and anthropogenic risks, within the context of the National Civil Protection Service's warning system.

Building the Audit: the phases

Auditing activities can be schematically grouped into the following four macro-phases:

1. **Context analysis:** this phase aims to observe the relevant characteristics of the internal and external environment in which the audited entity operates, as well as quantitative and qualitative elements that characterize it and that will be useful for properly conducting the risk exposure self-analysis activities. This phase, in turn, can be broken down into sub-phases:

    a. *Analysis of national and regional legislation,* internal regulations, and organizational documents, or—where applicable—Quality Management System documentation, to define the "expected conduct" of the various units within the organization, as well as of the individuals within these units. This analysis ultimately aims to detail the organization's activities at all regulatory levels, including internal ones consisting of regulations or service documents;

    b. *Analysis of the organization's* specific structure, that is, the specific organizational and management methods adopted, and the tasks assigned to assigned personnel. This analysis aims to reconstruct the relationship between "who" must perform a certain task and "what" must actually be performed. Indeed, it involves reconstructing the "guarantor positions" and, among the various parties involved (employer, manager, supervisor, employee, consultant, etc.), identifying the "guarantors" of the legal assets protected through the overall activities carried out by the audited organization.

    Analyses a) and b) also allow for the *evaluation of the adequacy of internal processes,* possibly also in comparison with some *case histories* and the documentation that codifies them.

    c. For some audited entities, given their significant involvement in certain legal proceedings, a *detailed analysis of the relevant material was also conducted.* This analysis allowed—empirically in these cases—both the clarification of legal issues relating to specific conduct of the operator

and/or the entity's activities, and the identification of possible specific remedial measures.

2. **Risk area mapping:** This is a process that allows for the identification and assessment of an organization's potential risks, based on its current state. Specifically, with regard to Functional Centers, the mapping highlights the risks to which the organization is exposed in carrying out forecasting activities, based on the assigned skills and responsibilities. The mapping process aims to highlight and, in any case, draw attention to how certain activities, encompassed by specific risk areas, can lead to "system errors" and "individual errors," with related organizational deficits in the former case and, in the latter, specific personal responsibilities related to the performance of the activities specific to each type of operator, including the various guarantor roles and the methods of coordination and interaction between them. At this stage, the cooperative nature of the activity emerges, as compiling the document explicitly involves a dialogue between the auditor—who develops risk assessments based on their desktop review—and the auditee, who provides their own "counter-arguments" in the form of actual contextual considerations. The comparison between the former and the latter determines the need to propose, already at this stage, mitigation/reinforcement actions or further investigations into the potential criticality identified.

3. **Quantifying risk exposure:** considering the frequency with which an error can occur and the extent of the damage it can cause the risk is assessed in relation to the identified aspects, areas, and contexts. This is done through the application of consolidated and replicable objective methodologies, yet still adapted to the specific nature of the organization being examined.

4. **Mitigation actions:** The auditing process concludes with the identification of possible improvement actions, based on the mapping conducted in the previous points. To support this, the CIMA Foundation will identify several national and international best practices. These actions typically involve limited human and financial resources and, in any case, aim for their sustainability.

Phase 1: Context analysis

The contextual analysis consists, in brief, of conducting a review of the sectoral regulations, both national and regional, as well as the internal procedures of the audited entity, to develop an initial overview of the duties and responsibilities of those responsible for forecasting, monitoring, and communicating the expected risk scenarios within the jurisdiction. The first phase of the analysis, therefore, focuses solely on those aspects of interest to the entity; therefore, the first phase is not intended to summarize a comprehensive analysis of the entire regulatory framework of the National Civil Protection System, not even its local branches.

The work therefore takes the form of a "desk" analysis; however, the methods used to identify the responsibilities and reference figures for the CF's processes, based on the legislation and documentation examined, likely reflect the modus operandi observed by

the Judicial Police appointed by the Investigating Magistrates in the context of an investigation into alleged unlawful acts attributable to personnel of the agency responsible for forecasting and warning.
The analysis, at this stage, is therefore aimed – using the methods described above – at identifying the product responsibilities that lead to the issuing of alerts and at identifying the parties burdened with such responsibilities based on current regulations and the documentation provided, and in particular:

- national legislation (the constitutional framework and primary legislation, secondlevel national legislation);
- regional and local legislation and the internal procedures of the Institution. The context analysis therefore constitutes only the necessary premise and the starting point of a much more detailed study which, by analyzing the expected behaviors and identifying the so-called "guarantee figures", intends to finally arrive at the prefiguration of actions to improve the system with a view to improving the efficiency of the specific Organization, of the Service generally understood, and of mitigating the Operator's risk.

Phase 2: Mapping of risk areas

The mapping of risk areas consists of an initial introductory section, aimed at providing essential information regarding "professional risk," with reference to the criminal risk for those assigned to operate in the sector in question, and a subsequent detailed analysis of the individual processes (or, more likely, parts thereof) deemed at risk. The first part of Phase 2 is generally structured as follows:

- general framework of civil protection activities and related professional risk (civil, criminal, reputational);
- sharing a glossary related to or the definition of crime.
    - the positions of guarantee and the participation of people in crime
    - the definition of guilt.
    - the distinction between error and system error.
    - Risk profiles for the institution's operators.

As already noted, the outcome depends on collaboration between entities that, albeit in different capacities and with different functions and responsibilities, belong to the National Civil Protection Service: the auditor, a multi-risk and multi-disciplinary center of expertise, and the audited entity, with operational functions within the regional civil protection system, particularly in the early warning segment. Therefore, to improve the efficiency and effectiveness of the agency's performance and, where appropriate, strengthen its security, verification, and procedural control measures, the auditing process must be characterized by the broadest possible dialogue between the parties, with clear discussion. For this reason, the applied methodology requires—in the second part of Phase 2—the auditor to propose "risk sheets," which identify potential risk areas, as deemed possible following joint reconnaissance. More specifically, it is important to point out that

the aforementioned factsheets are the result of a detailed work which, in its first draft and based on a scheme proposed by the CIMA Foundation, originates from the context analysis, from the considerations in the introductory part of this Phase, as well as from visits held at the institution being studied to directly evaluate its operations both under "ordinary" conditions and during an event [1].

The assessments by CIMA Foundation researchers are then formalized in risk assessment sheets. This initial version consists of information describing the identified criticality, the applicable legislation, the type of error, and the reason for highlighting a specific aspect. This is where the input from the auditee's operators and key figures comes in, allowing them to complete the section dedicated to so-called "contextual considerations," similar to the legal counterarguments to a hypothesis formulated by the opposing party (in this case, CIMA). The resulting discussion typically requires one or more subsequent meetings, which are necessary to further explore and clarify mutual positions regarding a potentially critical aspect. This phase, crucial for determining the "algebraic sum" of the auditors' assessments and the procedural, formal, and operational rationale of the entity being analyzed, leads to the final draft of the report, which, at this point, may include a section dedicated to "prospects and subsequent actions" for potential risk treatment. It is precisely from the outcome of this discussion that the opportunity, and sometimes necessity, of additional actions regarding a specific potential criticality becomes apparent. In any case, the critical aspect that emerges is incorporated—as the audit progresses—into "in-depth questionnaires" for the organization's staff, specifically for the purpose of providing empirical feedback.

Phase 3: Quantifying risk exposure

Finally, for the overall assessment of the final risk (the failure or incorrect prediction of the effects on the ground, the total or partial "failure" to perform the functions for which the entity is responsible, etc.), it is necessary to proceed with the quantification of the risk exposure, through Phase 3.

The proposed analysis model is divided into the following tasks:

- setting up the risk model
- risk appetite
- identification of the sample of subjects to be interviewed with a questionnaire
- creation of the risk assessment questionnaire
- administration of the questionnaire
- analysis of the questionnaire results and creation of the risk model.

[1] For these purposes, an event is simulated to reconstruct the expected modus operandi in an alert regime or at least in an operational phase of attention.

Setting up the risk model

From the analysis of the main characteristics of the activities carried out for risk assessment at the macro-procedural scale, the following "homogeneous risk areas" are identified:

1. Employee risk
2. Work organization risk
3. Risk general rules
4. Risk of adequacy of dedicated equipment
5. Risk of relationships with external parties.

For each risk area, several aspects to be assessed ("risk aspects") are identified, represented in questions to be submitted to the pool of operators of the regional civil protection system deemed significant.

Each aspect is assigned a weight, which serves to quantify the significance of the potential impact; the weight ranges from 1 (least relevance) to 5 (most relevance). The determination of the weights, based on the adopted practice, involves a collegial meeting between the CIMA Foundation and the auditee, in two phases: first, the weight is proposed by CIMA and then adjusted based on the considerations provided by various stakeholders within the auditee.

The weight assigned to the different aspects, calculated as described, is then normalized so that the sum of the weights of all the aspects provides - for each risk area - a value equal to 100.

Following administration, multiplying the score obtained from the questionnaire responses for each aspect by its normalized weight yields the actual score for that aspect. Adding the actual scores for all appropriately weighted aspects yields a numerical value (between 0 and 1000) to be used to classify the risk of the homogeneous area.

Risk appetite (risk propensity)

The weight range [0-1000] of the risk areas is divided into 5 risk levels:

- High [0-200];
- Medium-high [201-400];
- Medium [401-600];
- Medium-low [601-800]; − Low [801-1,000].

Given the nature of the structures audited to date, a medium-low risk propensity is considered acceptable, categorized into Low and Medium-Low risk levels, i.e. a risk value of no less than 601. The score represents the average of the scores of the individual responses for which the following are assigned:

- 10 points for a “compliant” response (i.e. in line with the defined operating procedure or with the expected level of knowledge for a given process or phase of it)
- 5 points for a doubtful answer

- 0 points for a non-compliant response (i.e. not in line with the defined operating procedure or with the expected level of knowledge for a given process or phase of it).

Although the result produces an average score for the single risk area intended to identify the level of risk among the 5 classified, the precaution was taken to examine in depth each single aspect of any risk area that has an actual score lower than 6 [2].

The verification of individual aspects with a score lower than 6, conducted as described above and referring to the "Risk Mapping Detail Sheets", returns one of the following results:

a. unfounded alert;
b. well-founded alert for which it is foreseeable for the final phase of the Project to indicate improvement actions or risk mitigation;
c. well-founded alert for which further investigation is deemed necessary, including through an internal audit.

The result must also consider the answers given to the control questions contained in the questionnaires, as well as the considerations of the specific context analysis and the mapping of critical issues carried out previously.

It's worth noting that some sets of questions, by their very construction, do not provide answers that are “compliant” or "non-compliant." This is the case for risk aspects that investigate highly subjective factors, such as, for example, the attitudinal consequences ("greater caution") resulting from previous legal actions involving the entity for performance or procedural reasons. In cases such as those mentioned, the subsequent analysis, based on the result achieved, highlights, where appropriate, weighty issues that may require further investigation upon completion of the analysis.

Identifying the sample of subjects to be interviewed

The overall and, above all, objective assessment used to determine the optimal pool of resources to be drawn upon for the administration of the questionnaire is based on verifying the presence of all the professional skills required to issue warning products for civil protection purposes (including those present in services external to the Functional Centre, but relevant to the product produced by it [3]), the estimation of hydrometeorological forces, or the expertise in monitoring and surveillance within the entity being analyzed. Adopting this approach is, in fact, an effective tool for ensuring a strategic and comprehensive approach to risk mitigation and for verifying the effectiveness and adequacy of existing risk controls.

[2] This foresight is reflected - essentially as a result of the same - in possible specific "reinforcement/improvement actions" that are finally suggested to the institution to provide a possible solution to the aspect that obtained a score lower than 6, considered an indicator of possible critical issues.

[3] The reference is to the IT area, i.e. to procurement or administrative-management areas that determine, directly or indirectly, the levels of service provided by the entity subject to audit.

Development of the risk assessment questionnaire

As anticipated in the previous paragraphs, the questions that make up the questionnaires are formulated taking into consideration:

i. the different stages of the process

ii. the different aspects of the risk areas, considered both in terms of probability and impact and in terms of evaluation of the existing internal control system

iii. the roles and responsibilities of the subjects involved in the various phases of the process.

For better management and comparability of results, it is generally considered preferable to prepare a series of restricted questions, which only allow for closed answers (YES/NO, ALWAYS/NEVER, etc.), to which an intermediate or doubtful option (DON'T KNOW, IMPROVEMENT/S, etc.) has sometimes been added, if the question makes this option plausible.

Similarly, it is common practice, in addition to questions aimed at ascertaining the existence of a risk, to follow up with one or more in-depth questions on the same aspect—called "control questions"—to ensure the correct interpretation of the question posed. It is important to emphasize that for each question ("risk aspect"), a free-text notes field is available through which the individual surveyed can enter additional considerations to supplement their response, in order to further detail elements not deducible from the predetermined answer options.

Administration of the questionnaire

Given the collaborative nature of the proposed approach, the questionnaire is being prepared by the CIMA Foundation, with subsequent validation by the audited entity to ensure the questions are understandable.

We then move on to the actual administration phase, taking care to precede it with a general introduction to the selected operators and officials to highlight their objectives and working methods.

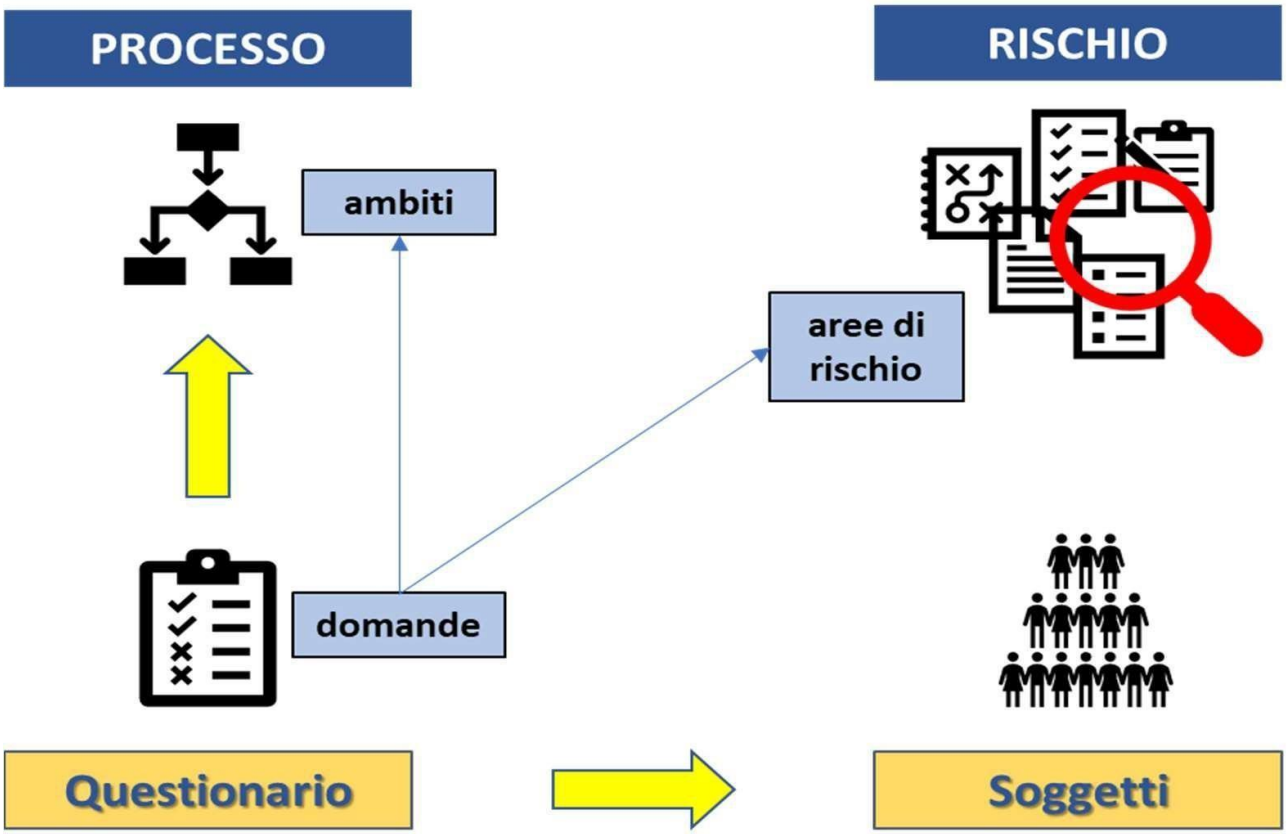
The questionnaire is administered anonymously to ensure maximum confidentiality and, therefore, the operator's ability to be as transparent and open as possible in their responses. Finally, the questionnaire with the aggregated results is made available to the entire working group.

At the end of this activity, the auditor's knowledge dataset can be considered complete, and it is possible to proceed with the evaluation of the questionnaire responses, which results in the creation of the risk model and risk treatment.

Analysis of the questionnaire results and creation of the risk model

The analysis of the questionnaire results is carried out by the CIMA Foundation and forms the basis for proposals for improving/strengthening the Structure or for risk mitigation. Each response is assigned a score using a predefined scale. Sometimes, the scores assigned

to certain responses to specific aspects are adjusted based on the comments entered by the operators in the questionnaires.
Considering that each aspect is described by multiple questions, the score for the same is obtained by adding the scores of the individual questions relating to it and dividing the sum by the number of questions, in order to obtain the average value (by construction between 0 and 10).
The score of the individual questions provides further detail for the risk assessment of the various aspects in order to identify the possible need to apply mitigation measures, as better developed in the next paragraph.



Process risk analysis scheme using questionnaire

Treatment of the score assigned to the answers for each question of the questionnaire

Risk treatment

Risk treatment formalizes the conclusions drawn from the methodology described above. Specifically, the results obtained in individual Risk Areas are detailed to allow for the implementation, where deemed appropriate and/or significant, of specific risk treatment actions depending on the level of criticality encountered (and thus, we will speak of "mitigation or coping actions" for high and medium-high risk, or more specifically and prospectively, "reinforcement/improvement and in-depth analysis actions" for mediumlow and low risk). While this paradigm is applied to risk aspects that achieve scores below a predetermined minimum compliance threshold, aspects that, although by their nature "unimportant," require in-depth analysis within the audited organization are often analyzed in detail. It is also not uncommon for auditors to recommend additional internal fact-finding action for "significant compliant" risk aspects, i.e., those procedural or management elements that, despite meeting the minimum threshold, have nevertheless highlighted potential ancillary or accessory criticalities (for example, established knowledge of practices that, although sanctioned by internal operating instructions, are exceeded or bypassed in the exercise of a specific function).

Comparative analysis of the mapping of risk areas: residual risk

The risk mapping process, which resulted in the preparation of risk sheets, identified several potentially critical aspects and, as such, were susceptible—as mentioned—to further investigation. At this point in the process, it was deemed appropriate to compare the findings from the in-depth risk assessment with the sheets. This additional step is necessary to determine whether and how residual risk factors arising from the juxtaposition of general considerations—expressed by F. CIMA—and contextual considerations—shared by the audited entity—are confirmed or neutralized by the results of the in-depth questionnaires. Specifically, this additional cross-checking across different levels within the audited entity may highlight the misalignment between the perceptions of management and operational levels *regarding* the efficiency of processes, tools, and operating practices, or their knowledge.

Overall risk

Finally, the final step in risk quantification consists in appropriately composing the resulting criticality levels for each aspect, scope, and homogeneous risk area into one or more overall indicators, capable of highlighting the risk associated with the process.

The criteria that could potentially be adopted are listed below:

1. Maximum caution: the overall risk (or risk range) is equal to that of the highestrisk area. This method, which is readily applicable and requires no calculations, has the advantage of immediately highlighting the most critical scenario that could occur, i.e., the existence of at least one "high" risk area capable of affecting the overall risk level.
2. Arithmetic mean: the overall risk is equal to the arithmetic mean of the risk scores of the individual areas. The arithmetic means have the property of considering the different risk bands equivalent in terms of their weight in determining the overall risk, but this may not correspond to the perception, derived from experience, which tends to give greater weight to high risk levels. For example, the presence of a

"high" risk area is offset by a "low" risk area, thus determining an overall "medium" risk. This effect does not reflect the true composition of the risk levels.

3. Weighted average: the overall risk is equal to the weighted average of the risk scores of the individual areas. In this case, assigning appropriate weights to the risk bands can more faithfully reproduce the expected outcome, namely that the overall risk tends to be more influenced by the highest-risk areas, without significant "compensatory effects" between areas with different risk levels.
4. hybrid approach: method 1 is combined with method 2 or method 1 with method 3.

Ultimately, determining the overall risk level serves two purposes:

- the first is aimed at defining the general level of risk – be it reputational or administrative, civil and/or criminal liability – of the entire process faced by the Institution (and specifically intended as providing an expert risk assessment to a decision-maker in the field of alerts for civil protection purposes).
- the second aims to highlight how the different components of the process can be considered autonomous from each other or interconnected and ultimately how each of them demonstrates the canons of indispensability.

Although these findings are different—and have different implications after their calculation—it seems appropriate to begin with the second consideration made here. The analysis of the process in its various components was conducted through an in-depth analysis of all the steps leading to the production of forecasting products for civil protection purposes within the audited entity. This breakdown, conducted jointly by the various stakeholders in the audit project, was designed with the specific purpose of highlighting all the essential and, where identified, critical steps that comprise the process. To provide practical evidence of the above, it must be understood that there can be no truly efficient operational Service if it were to deprive itself of the necessary equipment or essential services for carrying out ordinary and extraordinary activities, or even of adequately trained personnel for the tasks required by regulations, disciplinary measures, and internal procedures (which, ultimately, obviously cannot be ignored).

Phase 4: Reinforcement, mitigation and coping actions

The analysis and assessment of potential procedural and operational criticalities within the analyzed entity concludes with the CIMA Foundation formulating "deepening," "strengthening/improvement," or "mitigation and coping" actions for minor, medium, or major criticalities, respectively. Comparative analysis of the findings from the risk area mapping and risk assessment activities typically highlights the existence of certain procedural, operational, and organizational aspects worthy of proposals aimed at improving the efficiency of the affected segments while simultaneously reducing their vulnerability.

For the benefit of the reader, some examples of these operational countermeasures are reported as formulated during audits conducted by the CIMA Foundation at regional structures of the civil protection system.

Inadequate responsibilities perceived by the opPCs	*The opportunity is recognized by an investment aimed at training - specifically in terms of responsibility - of the operator fleet, involving institutions and/or professionals in the sector such as the Higher School of Civil Protection* *Furthermore, it is recommended that training activities be based primarily on the analysis of real-life cases involving counterpart bodies from other regions in legal proceedings related to severe hydrometeorological events.*
Product documentation storage according to CAD criteria	*It is necessary for the institution to comply with the current legislation on the matter and with the Directive of the President of the Council of Ministers on civil protection alerts and public warning system IT – Alert of 5 February 2021, also considering the indications contained in the corresponding Risk Sheet* *(See summary document of the mapping of the*

	(at-risk areas). It is believed that an exchange of information with the Regional Administrative Court ... and with the Central Functional Centre of the DPC, as structures that have already addressed the issue, could be useful.

Operator substitution rules coding	*It is essential that the organization, when defining service levels with the contracting/service provider, agree on the procedures for defining replacements for personnel assigned to shifts who, due to force majeure, are unable to perform their work. It is therefore important to note that the alert is of greater relevance to the organization. The contractor/service provider is not responsible for the institution, which is not required to review the procedures for defining backups, except for the execution of the activities specified in the specifications within the timeframe and in the manner specified therein. It may, however, be useful, or even appropriate, to include this issue in the inspections and/or service audits normally performed by the institution with the contractor/service provider.*
Operating instructions are incomplete and non-standardized	*The CFMR recognizes the need to complete the ongoing review of the documentation available to operators on duty for monitoring and surveillance activities, ensuring its classification within predefined formal standards capable of, for example, meeting the minimum requirements outlined in the corresponding document (see summary document of the mapping of risk areas). As already highlighted in the document, it is appropriate to extend the same approach to the documentation related to forecasting activities. It could, however, be useful, or even just appropriate, to initiate a consultation and collaborative process with operators to draft the documentation in question in such a way as to make it more of a "heritage" of the organization.*
Relationship with external stakeholders	*It is considered appropriate to share the feedback mechanisms activated with the operators*

	from the body with stakeholders external to the structure and, if deemed relevant, of the outcome of such findings, promoting - where possible - a participatory approach aimed at improving the efficiency of products and procedures.

Schematic breakdown of the audit

Following the systematization of the auditing process as formulated above, it is possible to propose – also for the benefit of a possible "abstract" presenting the work itself – the following schematic *breakdown:*

The investigations, conducted by CIMA Foundation staff in collaboration with the auditee in the exercise of its forecasting, monitoring, and surveillance functions (aimed at supporting civil protection decision-makers), apply a risk-oriented process analysis method to all the processes managed by the entity, based on a mixed approach (empirical and expert-based), conducted through:

- *the specific context analysis in reference to the entire meteorologicalhydrological forecasting process, the organization and the risk control systems inherent in the activity.*
- *the application of a risk assessment model.*

The specific context analysis is conducted by mapping the specific activities that contribute to the overall process risk. This activity is based on the observation of the organization by an external entity (CIMA Foundation) as it carries out its activities from the perspective of "professional risk," with reference to the criminal risk for those involved in the service in question. The overall assessments made by the working group throughout the various phases of the activities have, from time to time, highlighted potential critical issues that were subsequently verified in consultation with the institution's technical staff. The residual critical issues are then incorporated into the in-depth questionnaires administered to the institution's staff: the results of the operators' responses constitute the final step in defining the significance levels for each of the highlighted risk aspects. The outcome of the comparison between i) the desktop review conducted by the CIMA Foundation, ii) the contextual considerations of the institution's managers, and iii) the targeted in-depth analyses drawn from the pool of operators and, where applicable, from representatives of functionally adjacent services and offices, allows the alerts to be classified as unfounded, well-founded with a need for further investigation, or wellfounded with a suggestion for reinforcement.
While the first type of alert does not provide grounds for suggesting strengthening actions, the second and third types usually outline—with a view to contributing to the strengthening of the structure—possible solutions aimed, from time to time, at consolidating procedures and processes or further investigating the existence of elements that do not conform to efficient operating practices.

Improved procedure within RETURN

Improvements already made during the Project

Audit Process Diagram

During the project, which aimed—as mentioned—to provide representation and systematicity to the auditing activity, some "examiners" and project partners, who were asked for their opinion on the comprehensibility of the activity in question, noted the lack of a coherent descriptive framework for the audit process, capable of representing its phases, operational logic, and interconnections. This absence made it more difficult to fully understand the evaluation process undertaken with the audited entity, especially for those less involved in the preliminary methodological phases.

In response to this observation, an explanatory diagram was developed and shared—as illustrated in the previous paragraphs—intended as a guidance tool capable of guiding the user through the various phases of the audit process. See Annex **0** at the bottom of this Deliverable.

The diagram is intended to facilitate the sequential reading of the planned activities, as well as highlight the logical and functional connections between the main stages of the audit, promoting a clear, coherent, and functional overview for the implementation of the procedures.

This contribution is considered particularly useful for the audited entities, but also for all those involved in the planning, analysis, and evaluation of the actions undertaken in risk forecasting, monitoring, and communication, as well as for the readers of this work.

Introduction to rules, tasks, and institutions

To facilitate understanding of the audit process and properly contextualize the information collected—even by inexperienced stakeholders or those with only a limited understanding of the early warning system—the “Examiners” and Partners emphasized the usefulness of an explanatory introduction to the auditee's institutional competencies and operational processes. This introduction should include not only activities directly related to the early warning system, but also the cross-functional functions and complementary responsibilities assigned to the entity where applicable.

Providing this preliminary framework responds to the need to:

- facilitate the reading of the evidence emerging from the audit, reducing the risk of subjective interpretations or interpretations unrelated to the actual operating context;
- enhance the role of the institution in the overall panorama of risk management and civil protection;
- improve the dialogue between auditors and auditees, basing the evaluation on shared and transparent assumptions.

This approach was initially tested during the launch of the most recent auditing activity at a Regional Functional Center (summer 2025): the introduction of a session dedicated to

describing the responsibilities, internal functioning, and main processes active at the audited entity allowed for a more accurate understanding of the dynamics analyzed in subsequent phases of the audit, contributing to the construction of a more informed, targeted, and participatory evaluation process.

Using concrete examples for legal terms

In line with what was highlighted in the previous points, some Project Partners and Examiners have emphasized how the introduction of practical examples relating to each phase of the Audit process represents a further facilitating element, particularly in promoting understanding by non-specialist readers or those from different disciplinary fields.

The targeted use of concrete examples – taken from previous experiences or simulations – allows for a more immediate clarification of the operational dynamics, evaluation logic and connections between the various planned activities.

An even more significant benefit is found with legal and administrative terms, which are often present in audit language and potentially cause ambiguity or conflicting interpretations. In this sense, associating a technical term with an explicit use case or plausible scenario facilitates decoding, contextualizes its concrete application, and significantly reduces the risk of misunderstandings, especially during the phases of assigning responsibility, reviewing compliance records, or assessing procedural deviations.

The systematic inclusion of examples could therefore become an integral part of methodological documentation, even in the form of an appendix or repertoire, contributing to the diffusion of a more accessible, transparent, and replicable audit culture.

Further improvements are to be made.

Lexicon

One of the main criticisms raised by some Civil Protection officials regarding the Audit concerns the inconsistent use of certain terms, which are used to indicate different concepts, generating confusion among non-experts. To address this issue, it would be appropriate to develop a shared vocabulary for the audited entity, thus promoting correct conceptual and operational guidance.

Terminological ambiguity is often one of the main obstacles to understanding and ensuring the effectiveness of complex processes, including auditing in the context of Civil Protection.

The ambiguity identified is, in particular, semantic: terms such as "vulnerability," "exposure," "risk," or "resilience," "areas," "tasks," "aspects," "processes," "risk areas," and "at-risk areas," often used without a clear conceptual distinction, can take on different meanings depending on the discipline or technical field in question. For example, what is considered "risk" within the civil protection system may not coincide with how it is used by a territorial planner or an institutional communicator. This overlapping terminology risks generating confusion, particularly among less experienced readers or those from different disciplines.

The creation of a specific glossary, shared among the stakeholders involved (auditees, auditors, technical and institutional stakeholders), would help establish a common language and reduce misunderstandings. This would accomplish the difficult task of precisely and unambiguously defining each of these terms, clarifying their operational meaning within the current methodological context. This clarification would not only make the document more accessible but also improve the consistency and transparency of the evaluation process.
This tool should specifically:

- contain short but precise definitions;
- indicate the context of use of the term;
- possibly report terminological variations in other disciplinary fields.

Leaving the vocabulary to the audited entity promotes operational autonomy and contributes to greater linguistic and conceptual awareness, which is also useful for communicating risk to the public with a view to subsequent updates to the analysis (follow-up).
The first attempt at drafting an "Audit Vocabulary" is presented in **Appendix 1** to this Deliverable, at the bottom of the text, and was developed by CIMA Researchers. The document has been validated by entities already audited, as it arose from the concrete need to reduce terminological ambiguities that had emerged during previous operational experiences. The goal is to provide a clear and shared reference tool that can support audited entities in correctly interpreting key concepts and improving their risk response and communication capabilities.

Risk weighting

This work has highlighted, among other things, the need to consolidate the "risk weighting" phase, probably the most problematic in terms of objectivity and robustness.

Furthermore, the accountability process for the structures responsible for forecasting, monitoring, and communicating Civil Protection risk—as illustrated in the "Poster" session of the 2024 Project Conference [4]—identifies the risk exposure quantification, or weighting, phase as the core of the audit. This phase is conducted using consolidated and replicable methodologies, appropriately adapted to the specific needs of the entity being examined. The medium- to long-term goal is to objectively strengthen this process by consolidating both the system of indicators, based on existing literature and practices, and the risk weighting techniques.

The risk assessment phase is a crucial step as it directly impacts the quantification of the level of criticality associated with each functional and thematic area, thus determining the overall effectiveness of the diagnosis and proposed corrective actions.

---

[4] M. Morando, M. Altamura, A. Gioia, M. Giambelli, L. Molini, F. Munerol, " *Dissemination Workshop - RETURN - Turin, 1-2 February 2024"* .

Currently—as described above—the risk assessment is conducted by assigning a weight to each of the aspects that contribute to defining the risk—represented by the questions in the "depth questionnaire." The weight, expressed on a scale from 1 (least relevance) to 5 (most relevance), is assigned jointly by the working group composed of CIMA researchers and representatives from the audited entity, based on predominantly qualitative and subjective assessments.

This approach, while based on expert consultation and dialogue, has some limitations in terms of objectivity, reproducibility, and comparability over time and across different institutions. It is therefore necessary to take targeted action to make this phase methodologically more robust, reliable, and transparent.

From this perspective, it is considered worthy to proceed with two lines of improvement:

1. Development of an objective weighting system

A first proposal is to introduce objective criteria to guide the assignment of weights to different risk aspects. These criteria could be based on measurable and comparable dimensions, such as:

- the presence of stringent regulatory obligations;
- the degree of exposure to legal liability (both personal and institutional);
- the frequency and severity of impacts observed in past experiences;
- the level of attention the topic receives at the level of national or international guidelines;
- the potential reputational or communication impact in the event of inefficiencies or omissions.

Codifying these criteria would allow weights to be assigned in a systematic and verifiable way, minimizing the influence of individual subjectivity and enhancing the experiential component gained from previous audits.

2. Overcoming the weighing logic and transitioning to a conformity assessment system.

Alternatively, or in parallel, a more radical transformation of the weighting phase could be considered, abandoning the weighting system in favor of a model that directly assesses the level of conformity of the responses provided in the questionnaires. The current system provides a simple tripartite scale (10 for compliant responses, 5 for uncertain responses, 0 for non-compliant responses), which, however, does not allow for a precise representation of the degree of maturity or approximation of the analyzed processes. During discussions with Examiners, Partners and colleagues, the adoption of a more granular evaluation scale was proposed, divided for example into five levels:

- No compliance
- Poor compliance
- Average compliance
- Good compliance

- Excellent compliance

For each level, clear and verifiable descriptive parameters would be defined, allowing for a more balanced assessment, geared toward learning and organizational growth. This approach could be further enriched by drawing on the corpus of responses and case studies collected in previous audits, from which reference models or qualitative thresholds could be extracted.

Such a development would have the dual benefit of increasing methodological consistency between different audits conducted over time or in different regions and enhancing the audit process as a tool not only for control, but also for supporting and empowering the assessed organizations.

To this end, given the large sample size subjected to auditing thus far, one development path involves the use of artificial intelligence tools for the mass analysis of results and the determination of multi-parametric and objectified weighting systems.

Conclusions

What is Audit in the context of Civil Protection?

The audit described above therefore constitutes a systemic and multidisciplinary evaluation methodology, developed by the CIMA Foundation, defined here in great detail and with proposals for improvement, aimed at:

- Analyze the legal liability profiles of National Civil Protection Service (SNPC) operators.
- Assess the regulatory and procedural compliance of complex structures (Functional Centers, Operations Rooms, etc.).
- Identify organizational, operational, and management criticalities that may generate legal, reputational, and functional risks.
- Propose improvement, mitigation, or reinforcement actions based on empirical evidence and direct discussion with the audited entities.

The approach is structured in four main phases:

- Context analysis: regulatory and organizational study to reconstruct tasks, responsibilities, and guarantee positions.
- Mapping of risk areas: identifying potential critical issues, developing risk assessments and engaging in dialogue with the organization.
- Quantifying risk exposure: administering structured questionnaires, building a risk model, and classifying risk.

- Risk treatment: definition of corrective actions, organizational reinforcements, and improvement proposals.

Proposals for changes and improvements to the procedure

The document outlines a comprehensive set of improvement guidelines, some already implemented and others in the proposal phase, which are listed below and subsequently - the most significant - explored in greater detail.

1. Extension of the Audit scope

- Audit not only of the Functional Centers, but also:
    - To the Operations Rooms, to verify the effectiveness and consistency of response procedures. o To the Regional Civil Protection Structures, with a focus on territorial planning and consistency with other sectoral policies (e.g., introduction of tools such as the SEA).

2. Methodological clarity and accessibility

- Descriptive diagram of the Audit process: introduced to facilitate the sequential understanding of the phases.
- Explanatory introduction to the rules, duties, and institutions: useful for clarifying the role of the audited entity and reducing misinterpretations.
- Systematic use of concrete examples, especially to clarify legal and operational concepts to non-specialist interlocutors.

3. Standardization of technical language

- Shared Audit Glossary: To reduce semantic ambiguity and promote interdisciplinary understanding. Includes working definitions, usage examples, application context, and explanatory notes.
    - Divided into categories: organization, methodology, tools, legal.

4. Strengthening the risk weighting phase

- Objective assignment of weights to risk aspects, based on:
    - Regulatory obligations or Legal responsibilities or Observed impacts or Reputational relevance
- Moving beyond the weighing logic: a proposal to move to a graduated conformity assessment system (none, poor, medium, good, excellent).
- Using artificial intelligence tools for massive analysis and building objective weighting models.

5. Transformative approach to control

- Overcoming the inspection vision of control.
- Promoting systemic and adaptive risk governance, oriented towards organizational learning.

- Control as a strategic lever for transparency, legitimacy, and innovation.

6. Operational and training actions

- Targeted training on legal liability, with analysis of real cases.
- Review and standardization of operating instructions, with the active involvement of operators.
- Improved document preservation, in accordance with CAD criteria and current legislation.
- Codification of staff replacement rules, especially in contracted services.
- Sharing feedback with external stakeholders to promote transparency and continuous improvement.

7. Inclusion of emerging and systemic risks

- Extension of control also to:
    - Non-traditional environmental risks (e.g., heat waves, droughts, biodiversity loss) o Cyber risks and information vulnerabilities (e.g. IT-Alert)
    - Organizational and reputational risks related to the ecological and digital transition

8. Enhancement of human capital

- Reviewing post-pandemic leadership, training, and evaluation models.
- Building resilient, motivating, and learning work environments.

Towards a risk governance based on systemic awareness and transformative responsibility

The above outlines precisely the attempt to move beyond the traditional concept of control, understood as an inspection tool aimed at identifying those responsible for a procedural discrepancy or deficiency, in favor of an advanced and systemic vision, in which control takes on the function of a strategic lever for continuous improvement, promoting transparency, and strengthening the organization's legitimacy among its stakeholders.
This epistemological transition is rooted in the awareness that contemporary organizations – primarily public ones or those that, by mission, must maintain a constant relationship with the public – are called upon to confront a set of structural and interdependent critical issues that exceed the boundaries of conventionally understood risk:

- Economic instability: Economic instability is a structural and interconnected global phenomenon, characterized by recurrent financial shocks, market volatility, and restrictive monetary policies adopted to contain inflationary pressures. The sudden increase in interest rates by central banks has had knock-on effects on public and private budgets, slowing strategic investments in infrastructure, innovation, and the ecological transition.

- Geopolitical instability: Geopolitical instability is a systemic risk factor manifesting itself through armed conflicts, diplomatic tensions, trade wars, and energy crises. The Russian-Ukrainian conflict, for example, triggered a profound energy crisis, forcing governments and local administrations to revise their procurement strategies and invest in renewable sources, which, however, exposed new logistical, technological, and diplomatic vulnerabilities. At the same time, tensions in the Middle East continue to impact global energy and commodity markets, while the rise in trade tariffs between major economic powers has further fragmented value chains, fueling uncertainty and protectionism.
- Climate emergency and ecological transition: Heatwaves, recorded with increasing frequency and intensity, are increasing the pressure on healthcare and civil protection systems year after year, highlighting the need for climate adaptation plans and cross-sector governance of environmental risk. Furthermore, the extremization of climate, resulting in the increased frequency of paroxysmal events, clashes with the difficulties that forecasting systems encounter in providing reliable estimates of impacts on assets and the population with sufficient spatial precision and temporal advancement, undermining the fundamental relationship of trust between institutions, scientific communities, and stakeholders.
- Redefining organizational culture and enhancing human capital: After the pandemic, many public administrations introduced hybrid work models, which required a rethink of evaluation, training, and leadership systems. The challenge shifted from simply managing personnel to building resilient and motivating work environments.
- Growing exposure to cyber risk and cyber vulnerability: the IT-Alert system, designed to promptly send alerts to citizens in the event of serious emergencies (e.g., natural disasters, industrial accidents, water crises), represents an important civil protection tool. However, its effectiveness is closely tied to the security of the digital infrastructures that support it. A targeted cyber-attack—for example, sabotage of the transmission network or manipulation of message content—could compromise the timeliness and reliability of the alert, generating confusion, panic, or underestimation of the risk. This highlights how cybersecurity is not just a technical issue, but a key component of institutional trust and operational resilience among the population.
- Technological acceleration and the impact of artificial intelligence: the introduction of AI algorithms to manage administrative procedures (e.g., automatic grant allocation or rankings) has raised ethical and legal questions about the transparency of decisions and liability in the event of algorithmic errors or discrimination.

These phenomena, due to their systemic and dynamic nature, cannot be fully managed using traditional methodological tools. They require a radical rethinking of the approach to risk, based on a logic of anticipation, measurement, and adaptation.

As Lord Kelvin warned, *"If you can't measure something, you can't improve it* ." And so, measurement becomes "the" essential prerequisite for acting on:

- Organizational resilience, understood as the ability to absorb shocks and regenerate

- Integrated sustainability, in its environmental, social and governance dimensions
- Technological and managerial innovation, as a proactive response to complexity • Multilevel accountability, towards judicial control and civil society

From this perspective, control is no longer seen as a retrospective exercise of censorship, but rather as a prospective device for learning and transformation.

Towards a governance of "traditional" and "emerging" risks

In a context marked by increasing complexity and interdependence, public oversight of its own activities is evolving into a forward-looking framework, geared toward organizational learning. This methodological and cultural repositioning allows for the expansion of the scope of analysis and the inclusion, alongside traditionally monitored risks, of emerging ones—such as heat waves, drought, and biodiversity loss. Furthermore, this also includes traditional risks, such as forest fires, which, despite having systemic and growing impacts, often escape full consideration by functional centers and civil protection agencies, creating social disaffection and a loss of credibility.

The challenge for the CIMA Foundation and projects like the PNRR-Return is therefore not only technical, but also strategic: it involves developing a comprehensive and adaptive methodology capable of identifying latent vulnerabilities and anticipating risk trajectories, integrating environmental, social, technological, and organizational dimensions. Such a methodology must be based on multidisciplinary analysis tools, predictive indicators, and governance capable of combining evaluative rigor and operational flexibility.

Within this framework, risk governance must be informed, i.e., based on a systemic and critical understanding of the interactions between risk factors; ethical, in the sense of being oriented toward the protection of common goods and intergenerational justice; and relational, capable of activating collaborative networks between institutional, scientific, and civic actors. Control, from this perspective, becomes an instrument of trust, a catalyst for collective learning, and a safeguard for shared responsibility.

Only through this reconfiguration will it be possible to address the challenges of the present and future, promoting a risk culture that goes beyond emergency management to generate resilience, sustainability, and systemic innovation.

Beyond Functional Centers: An Audit for Risk Governance and Territorial Coherence

The analysis of the auditing methodology and CIMA's experience, gained over ten years of auditing, highlight the urgent need to strengthen governance mechanisms within the civil protection system—and not just within the Functional Centers—with particular attention to risk management and, concurrently, planning. It is proposed to expand the scope of audits already planned for the Functional Centers, extending them to additional operational and decision-making hubs:

- to the Operations Rooms, to verify the effectiveness of the activation procedures, the timeliness of responses and the consistency between the protocols adopted at the local and national level;

- to the regional Civil Protection structures, with particular attention to the planning dimension.

Regional authorities could be encouraged to introduce integrated assessment tools, such as the Strategic Environmental Assessment (SEA) or similar, applied to civil protection plans to ensure greater consistency with sectoral territorial policies (transport, land use, environmental protection, urban development).

At the same time, the need to introduce a social evaluation of the audit product is highlighted, inspired by the recent guidelines adopted for ETS projects. This approach would aim to measure the social impact of risk management strategies and planning decisions, enhancing the involvement of local communities, the transparency of decisionmaking processes, and the ability to respond inclusively to local needs. Social evaluation would thus become a key tool for ensuring fairness, legitimacy, and sustainability of civil protection policies.

These proposals aim to promote a systemic and cross-sectoral vision of risk management, based on criteria of transparency, operational effectiveness, and territorial sustainability.

Annex 0 – "Audit Process Outline"

Quick Legend of the Phases

- **Phase 1: Regulatory and organizational study to reconstruct tasks and responsibilities.**
- **Phase 2: Identification of critical areas and discussion with the Authority.**
- **Phase 3: Objective risk measurement through questionnaires and models.**
- **Phase 4: Proposals for intervention, reinforcement or mitigation.**
- **Phase 5: Follow-up: re-analysis of the entity after several years**

Scheme


INIZIO AUDIT
Analisi normativa
(nazionale, regionale, interna)
Analisi assetto organizzativo
(figure di garanzia)
Eventuale analisi giudiziaria
(se rilevante)
FASE 1
Analisi di contesto
FASE 2
Mappatura delle aree a rischio
Inquadramento rischi
(penali, civili, reputazionali)
Redazione schede di rischio
(Fondazione CIMA + Ente)
Condivisione delle "considerazioni di contesto"
Costruzione risk model
(5 aree di rischio)
Somministrazione questionario anonimo
Approccio collaborativo continuo
FASE 3
Quantificazione del rischio
FASE 4
Azioni di mitigazione
Formulazione di azioni di mitigazione
(Fondazione CIMA)
FINE AUDIT
Nuovo audit
(allo stesso soggetto ad almeno due anni dal precedente)
Analisi dell'efficacia delle azioni di mitigazione
FASE 5
Follow-up

Annex 1 – "Audit Vocabulary"

Methodological introduction to the glossary

This glossary was created as a tool to support the reading and understanding of the Audit process as applied within the RETURN project, within the scope of the activities carried out by the CIMA Foundation.
During the implementation of the project activities, several stakeholders identified the need to clarify and standardize the technical and methodological vocabulary used in the documentation and in interactions between auditors and auditees. Terms such as *scope, aspect, process, risk area*, *risk sheet*, or *alert* , while formally recurrent, may be used with partially overlapping or variable meanings depending on the context. This can hinder a full understanding of the content by non-specialists or stakeholders with different disciplinary backgrounds.

To meet this need, the glossary was built through:

- the systematic analysis of the technical-operational documentation produced;
- the comparison with the partners and the audited entities;
- the detection of the most frequent linguistic ambiguities;
- the structuring into thematic sections to facilitate consultation.

Each entry is accompanied by:

- a concise and operational definition;
- an example of use taken from real or simulated situations;
- the reference to the stage of the audit process in which the term is used;
- an explanatory note that clarifies any areas of application or potential semantic ambiguities.

The objective is twofold: on the one hand, to strengthen terminological consistency and precision in audit activities; on the other, to promote transparency, replicability, and interinstitutional understanding of the proposed method.

Definition of categories

For ease of reference, the terms are divided into four main categories:

- **Organization:** includes concepts related to the structure, roles, responsibilities, and relationships between stakeholders within the civil protection system. It concerns the internal dynamics of the audited entity and its positioning within the institutional context. Examples: Stakeholder, Critical Rotation.
- **Methodology**: This category encompasses the terms that describe the audit's analytical and evaluative approach, the risk classification logic, the process phases, and the weighting criteria. This category shapes the audit's conceptual model. Examples: Risk area, Risk appetite .

- **Tools**: This includes the technical and documentary tools used during the audit, such as questionnaires, forms, templates, and data collection systems. These are the operational tools that translate the methodology into practice. Examples: Risk Sheet, In-Depth Questionnaire.
- **Legal**: This category includes terms derived from criminal, administrative, or civil law, which are relevant to assessing liability and legal risk profiles. This category is central to analyzing liability positions and regulatory obligations. Examples: Legal liability, Guarantee position.

Glossary

Organization

- **Operational backup**
  Mechanism for replacing staff in case of unavailability.
  Example: “Lack of operational backup rules generated an alert.”
  Reference: Phase 4 – Reinforcement Actions Note:
  May involve contracting or internal entities.

- **Feedback from stakeholders**
  Feedback received from external parties on the effectiveness of products or services. *Example:* "Feedback from stakeholders highlighted deficiencies in risk communication."
  Reference: Phase 4 – Participatory actions
  Note: Helpful for improving transparency and trust

- **Operational instruction**
  Document describing the execution methods of a procedure.
  Example: “The operational instruction for monitoring was found to be deficient.”
  Reference: Phase 2 – Risk Sheets
  Note: It must be standardized and shared among operators.

- **Stakeholder**
  External or internal subjects interact with the audited entity.
  Example: “Stakeholders were involved in the auditing process.”
  Reference: Phase 1 – Context Analysis
  Note: Includes entities, suppliers, citizens, other CFs.

- **Critical shift**
  Shift organization that puts service continuity at risk.
  Example: “Critical shift work has been flagged as a residual risk.”
  Reference: Phase 3 – Comparative Analysis
  Note: Often linked to staff shortages or uncodified rules

Methodology

- **Risk Scope**
  Thematic segment that aggregates critical aspects pertaining to the same function or area.
  Example: “The scope of 'dedicated instrumentation' includes aspects related to technical adequacy.”
  Reference: Phase 3 – Risk model
  Note: May contain multiple risk areas and aspects.

- **Risk area**
  Homogeneous aggregate of critical aspects evaluated in a unitary way.
  Example: “The area 'work organization' obtained a medium-low score.”
  Reference: Phase 3 – Setting up the risk model *Note:*
  Rated on a scale of 0–1000.

- **Risk aspect**
  Specific element to be evaluated within a risk area.
  Example: “The aspect 'document preservation' received a score of 4.” *Reference:* Phase 3 – Questionnaire and weighting *Note:* Each aspect is associated with questions and weights.

- **Risk communication**
  Process of informing and involving the exposed population. *Example:* "Risk communication was fragmented and non-standardized."
  Reference: Phase 1 – Context Analysis
  Note: Includes content, channels, and language used.

- **Compliance**
  Level of adherence to operational and regulatory procedures.
  Example: “The response was considered compliant and scored 10 points.”
  Reference: Phase 3 – Questionnaire Evaluation *Note:* Rated on a 0–10 scale.

- **System error**
  Critical issues arising from organizational or procedural deficits.
  Example: “The system error occurred in the management of duty shifts.”
  Reference: Phase 2 – Mapping
  Note: Distinct from individual error.

- **Risk perception**
  Level of awareness and understanding of risk among recipients. *Example:* "Risk perception has been influenced by previous legal events."
  Reference: Phase 3 – In-depth questionnaire
  Note: It can be measured and improved with training and dialogue.
- **Weighting**
  Assigning weights to risk aspects to determine their relevance. *Example:* "The weighting assigned a weight of 5 to the adequacy of the instrumentation."
  Reference: Phase 3 – Risk model
  Note: It can be objective or subjective.

- **Process**
  Structured set of activities, decisions, and information flows connected to a goal.
  Example: “The alert process is divided into six operational phases.”
  Reference: Phase 2 – Mapping of risk areas
  Note: Central audit object; can be broken down into tasks.

- **Residual risk**
  The portion of risk remains after the application of mitigation measures. *Example:* "The residual risk was confirmed by comparing the sheets and questionnaires."
  Reference: Phase 3 – Comparative Analysis
  Note: May indicate misalignment between management and operational levels.

- **Risk appetite**
  Acceptable risk appetite for the audited organization.
  Example: “The CF shows a medium-low risk appetite, consistent with its public function.”
  Reference: Phase 3 – Risk Quantification *Note:*
  Threshold value ≥ 601 on a 0–1000 scale.

- **Risk model**
  Analytical model for risk quantification and classification.
  Example: “The risk model has classified the 'external relations' area as medium risk.”
  Reference: Phase 3 – Analysis of results
  Note: Based on scores, weights, and normalization.

- **Risk treatment**
  Set of actions proposed to mitigate, strengthen, or deepen critical issues.
  Example: “The risk treatment included improvement actions at the individual resources level.”
  Reference: Phase 4 – Concluding actions
  Note: Can be operational, formative or procedural.

- **Task**
  An operational unit of the audit process, corresponding to a phase or subphase.
  Example: "The 'questionnaire administration' task precedes the construction of the risk model."
  Reference: Phase 3 – Schematic Breakdown
  Note: Can be used to describe specific activities.

Instruments

- **Alert**
  Report on potential or confirmed criticality that emerged during the audit.
  Example: “The CAD documentation alert was confirmed and triggered corrective action.”

Reference: Phase 3 – Check score <6
Note: It can be unfounded, well-founded, or needs further investigation.

- **Contextual considerations**
  Counterarguments provided by the audited entity in response to the risk sheets.
  Example: “Contextual considerations have scaled down the proposed alert.”
  Reference: Phase 2 – Risk Sheets *Note:*
  Like legal counterarguments.

- **Desktop review**
  Preliminary document analysis conducted by the auditor.
  Example: “The desktop review highlighted critical issues in product preservation.”
  Reference: Phase 2 – Mapping
  Note: Basis for the preparation of risk sheets.

- **Depth questionnaire**
  Survey tool administered to operators to assess risk aspects.
  Example: "The questionnaire revealed a lack of knowledge of operating procedures."
  Reference: Phase 3 – Questionnaire Administration
  Note: Includes closed questions and free notes field.

- **Risk sheet**
  A document describing critical issues, regulations, type of error, and corrective actions.
  Example: "The risk sheet highlights the failure to store products according to CAD."
  Reference: Phase 2 – Risk Sheets
  Note: Also includes counter-arguments from the audited entity.

Legal

- **Specific fault**
  Violation of technical rules or regulations that define the required conduct.
  Example: "Specific negligence was assessed based on the technical rules violated."
  Reference: Phase 2 – Legal Glossary
  Note: Central to criminal proceedings; distinct from general guilt.
- **Concurrence by omission**
  Passive participation of multiple parties in an unlawful act due to failure to act.
  Example: “A conspiracy of omission between multiple guarantor figures has been hypothesized.”
  Reference: Phase 2 – Mapping of responsibilities
  Note: Relevant for audits with criminal implications.

- **Guarantee figure**
  Entity responsible for the protection of relevant legal assets within the system.

Example: “The CF manager is the person responsible for ensuring the alert is issued correctly.”
Reference: Phase 1 – Context Analysis
Note: Includes managerial, technical, and operational roles with expected responsibilities.

- **Guarantee position**
  Role that entails obligations to protect significant legal assets.
  Example: “The CF manager holds a position of guarantor for the alert.”
  Reference: Phase 1 – Regulatory Analysis *Note:* Fundamental for legal liability.

- **Legal responsibility**
  Obligation to answer for one's actions in civil, criminal, or administrative courts.
  Example : “The audit highlighted legal liability issues for the CF manager.”
  Reference : Phase 1 – Regulatory Analysis
  Note : This may concern both natural people and the entity as a whole.