D1.1.2. MAPPING OF THE GOVERNANCE AND DECISION-MAKING STRUCTURES ACTIVATED DURING AN EWS ALERT

Author: Innovation and Development ltd
Date: 15/12/2025

Table of Contents

1. Executive Summary

Document *Mapping of the governance and decision-making structures activated during an EWS alert* provides an evidence-based overview of how Early Warning System (EWS) alerts are governed and operationally managed across the Interreg Italy–Croatia Programme Area under the REALIST project. The deliverable maps the "as-is" decisional architecture activated during an alert, with a specific focus on decisional-tree schematisation and the main roles and responsibilities connected to partners' operational EWS arrangements. In line with REALIST objectives, the mapping supports harmonisation, upgrading, and interoperability of EWS-related governance and procedures across the Adriatic area by establishing a shared and comparable baseline.

The deliverable consolidates information from partner self-assessments collected through a standardised questionnaire (covering all partner inputs available at the time of compilation, including those received after the initial consolidation cycle) and from official publicly available sources (institutional frameworks, published procedures, and relevant legal/institutional references). The analysis follows a structured approach to ensure consistency and comparability across territories, including terminology harmonisation and internal coherence checks. Only information available in the collected sources is reported; where specific details were not available, this is indicated as "Not specified in available sources" to avoid assumptions and preserve traceability.

This governance mapping covers the full alert lifecycle, from the first technical signal to the deactivation of operational arrangements, including:

- Detection and triggering (monitoring, forecasts, thresholds, field reports);
- Validation and assessment (technical verification and interpretation of expected impacts);
- Classification of alert level (assignment of severity category/level);
- Decision and authorisation (formal approval to issue, update, escalate, downgrade, or terminate an alert);
- Dissemination (institutional notification, public warning, and last-mile arrangements);
- Activation and escalation (activation of operational centres and coordination structures; mobilisation of response actors);
- Update and termination (update cycles, deactivation decisions, post-alert reporting and learning processes).

In addition, the deliverable highlights the governance interface to public warning, clarifying which actors are authorised to communicate to the public and how dissemination responsibilities relate to the technical and operational command chain. Where relevant, it also captures how governance arrangements connect to operational coordination structures (e.g., control/operations rooms, civil protection coordination bodies) and how escalation is managed across levels (local–regional–national) within the Programme Area context.

To support both operational understanding and cross-territory comparability, this document delivers:

- A generic decisional-tree model describing the standard governance functions activated during an EWS alert, structured as a stepwise lifecycle applicable across Programme Area contexts.
- Partner governance fiches presenting, for each participating territory/system, the key decision points, responsible institutions, escalation arrangements, and public warning interfaces using a consistent minimum dataset.
- A comparative benchmarking synthesis assessing governance arrangements through practical dimensions relevant for REALIST objectives, such as role clarity, decision efficiency, coordination and escalation, traceability, and interoperability-relevant touchpoints.

The mapping confirms that, across different institutional settings, EWS alert management typically relies on a sequence of governance functions: technical detection and validation, formal classification and authorisation, structured dissemination, and activation of operational coordination and response arrangements. At the same time, the mapping highlights that differences in terminology, alert-level interpretation, distribution of decision authority, public warning interfaces, and escalation practices can reduce comparability and may create friction points for cross-border coordination. These findings establish a shared baseline for identifying where procedural alignment, clearer interfaces, and better-defined handovers can strengthen preparedness and responsiveness across the Adriatic area.

Mapping of the governance and decision-making structures activated during an EWS alert is designed as a baseline for subsequent REALIST work on identifying weaknesses and missing elements and defining improvement directions and interoperability opportunities. It provides a structured, evidence-based foundation for the development of harmonised recommendations and shared governance principles for upgrading EWS-related decision-making and coordination in the Programme Area.

2. Introduction

2.1 Purpose of the document

This deliverable provides a structured mapping of the governance, chain of command, and decision-making processes activated when an Early Warning System (EWS) issues an alert within the territories represented by the project partners in the Interreg Italy–Croatia Programme Area. The purpose is to document the "as-is" decisional architecture of EWS alert management, with a focus on:

- Decisional-tree schematisation: how an alert is triggered, validated, classified, authorised, disseminated, and managed over time (including update, downgrade/escalation, and termination), and which coordination structures are activated in response;
- Main roles and responsibilities: which organisations and functions are responsible and/or accountable for key decisions (e.g., issuing or authorising an alert, approving public messages, activating operational centres, escalating to higher levels, and terminating the alert);
- Operational clarity and efficiency: how clearly the command chain functions during time-critical situations, and where bottlenecks, overlaps, or ambiguities may affect timely decision-making and coordinated action.

The mapping is designed as a baseline for subsequent REALIST activities on benchmarking, identification of governance gaps and missing elements, and formulation of harmonisation and upgrading recommendations within the Programme Area.

This deliverable focuses specifically on governance and decision-making structures activated during an EWS alert. The complementary deliverable Mapping report on existing EWS provides the broader mapping of EWS features, links to legal frameworks, actions and communication fluxes, and inventories of instruments and IT platforms.

2.2 Scope and Programme Area coverage

The The mapping covers operational governance practices implemented within the Programme Area across project partner territories in Croatia and Italy, based primarily on partner-provided information collected through a structured questionnaire and consolidated into a common reporting format. Where relevant, partner inputs are complemented by official publicly available sources (institutional frameworks, published procedures, and legal/institutional references). The mapping reflects the full set of partner inputs available at the time of compilation, including those received after the initial consolidation cycle.

The deliverable maps structures and processes activated during an EWS alert across the full alert lifecycle:

1. Detection and triggering (monitoring, forecasts, thresholds, field reports);
2. Validation and assessment (technical validation of inputs and interpretation of expected impacts);
3. Classification of alert level (assignment of severity category/level);
4. Decision and authorisation (formal approval to issue, update, escalate, downgrade, or terminate an alert);
5. Dissemination (institutional notification, public warning, and last-mile arrangements);
6. Activation and escalation (activation of operational centres and coordination bodies, and mobilisation of response actors);
7. Update, stand-down, and learning (update cycles, deactivation decisions, post-alert reporting, and lessons-learned practices where described).

The mapping includes institutional alerting flows (who informs whom, through which official channels) and the governance interface to public warning, i.e., which actors are authorised to communicate to the public and under which procedures.

The analysis highlights interfaces between technical EWS actors (e.g., functional centres, hydro-meteorological services) and civil protection and responder organisations responsible for preparedness and response. It covers competent authorities and operational stakeholders involved in alert-related decisions within partner territories, including (as applicable): forecasting/functional services, civil protection bodies at national/regional/local levels, operational rooms/centres, emergency communication and dispatch functions (e.g., 112), municipalities, responder services, and, where explicitly documented, relevant operators of critical infrastructure.

Where a project partner is not a competent authority for issuing alerts (e.g., organisations with primarily development, coordination, research, or support roles), their contribution is captured as an interface/support role in the governance chain rather than as an “alert issuer”.

To keep the deliverable targeted, the following elements are treated only at a high level here or are addressed primarily in the *Mapping report on existing EWS* and subsequent work packages:

- Detailed technical descriptions of EWS components (sensors, models, platform architectures, data pipelines);

- Comprehensive assessment of quantitative performance metrics (beyond what is needed to interpret governance and decision points);
- Complete tactical field procedures and operational response plans (except where they are directly triggered or authorised by the alert decision chain).

This deliverable reflects the information available in the collected sources at the time of compilation. Where elements are not available in partner inputs or are outside a partner's mandate/visibility, they are indicated as "Not specified in available sources" to avoid assumptions and ensure traceability.

2.3 Definitions and terminology bridge (Croatia–Italy)

To ensure consistency across institutional contexts, the following terms are used throughout this deliverable:

- Early Warning System (EWS): the operational set of organisations, processes, and tools that detect, assess, and communicate impending hazards or impacts and support decision-making for protective actions.
- Alert: an official statement indicating a defined level of expected hazard impact within a specified area and timeframe, triggering predefined decision and coordination steps.
- Alert level / severity level: the classification of the alert into graded levels (e.g., phases or colour codes) used to trigger different degrees of readiness and response.
- Competent authority: the organisation(s) legally mandated to issue and/or authorise alerts within a territory.
- Functional centre / technical issuing body: the entity responsible for technical assessment and, in some systems, for issuing or co-signing alerts (e.g., forecasting and monitoring services, functional centres).
- Operational centre / operational room: the body responsible for operational coordination and for activating procedures, resources, and inter-agency coordination during alerts.
- Chain of command: the structured set of decision-making and escalation relationships activated during an alert, including authorisation pathways and delegation rules.
- Decision point (gate): a formal step where an authority validates, authorises, escalates, updates, downgrades, or terminates an alert-related action.
- Dissemination: transmission of alert information institutionally to authorities/responders and to the public (public warning), including last-mile communication.
- Escalation: the process of moving to higher coordination and command levels due to increased severity, uncertainty, or operational needs.
- Last-mile public warning: communication of actionable guidance to the population at risk through channels that ensure reach and comprehension (e.g., municipal channels, mass media, SMS, sirens, apps).

- Decision log: a structured record of alert-related decisions (time, decision-maker, basis, dissemination channels, versioning), supporting accountability and after-action learning.

Alert level terminology differs between Italy and Croatia and may also vary across Italian regions. To enable comparison without forcing artificial equivalences, this deliverable applies a two-layer approach:

- Each partner fiche reports the native/local terminology used in the territory (e.g., phases or colour codes).
- For comparative purposes, local levels are additionally mapped, where possible, to a generic four-band severity scale used only as an analytical reference to support cross-case discussion:

L0 – Monitoring / Information: routine monitoring; no activation beyond standard operations.

L1 – Advisory / Attention: increased attention and limited preparedness actions.

L2 – Warning / Pre-emergency: significant expected impacts; activation of coordination structures and preparedness measures.

L3 – Emergency / Severe warning: high/very high expected impacts; full activation of operational command, intensive coordination, and response readiness.

Because institutional roles and activation thresholds differ by territory, this deliverable does not assume that labels are identical across systems; instead, it documents who decides what at each level and what structures are activated.

Meaning of "alert" in the Italian and Croatian contexts (operational interpretation)

In the Italian partner territories, an alert ("allerta") typically refers to a structured, graded process in which technical assessment and civil protection governance interact to issue warnings and activate regional/provincial/municipal coordination structures and predefined procedures. In the Croatian partner territories, an "alert" is generally understood as a warning or notification derived from technical assessment (e.g., hydro-meteorological warnings) and operationalised through civil protection and emergency communication structures, triggering preparedness and response coordination at regional and local levels. This deliverable captures both contexts through decision points, authorisation pathways, escalation rules, and activation structures, enabling comparison despite differences in institutional terminology.

3. Methodology

3.1 Preparation phase

The preparation phase established a common methodological basis to ensure consistency and comparability across partner territories. It included: definition of the governance and decision-making scope of this document in line with Activity 1.1 Mapping and benchmarking of existing EWS, policies and platforms requirements; development of a standardised data-collection instrument (EWS Mapping Questionnaire) with dedicated sections addressing chain of command, decision points, and public warning interfaces during alerts; identification of focal points in each partner institution responsible for completing the questionnaire and coordinating, where relevant, with competent authorities (Civil Protection, emergency management structures, hydro-meteorological services); and development of a common consolidation format ("Partner fiches") to support structured synthesis and benchmarking.

To support cross-territory benchmarking, the preparation phase also defined a uniform minimum dataset for all fiches (decisional-tree steps, activation structures, and key responsibilities), and a terminology bridge to map local institutional labels to functional governance categories used consistently throughout the document.

3.2 Data collection approach

This deliverable was developed under Activity 1.1 *Mapping and benchmarking of existing EWS, policies, and platforms*, which foresees a structured data-collection process to consolidate information on operational EWS governance arrangements within the Programme Area, with a specific focus on the chain of command and decision-making during an EWS alert.

In line with the Work Plan, Partner ZADRA NOVA coordinated the data collection and consolidation process for this document and the complementary deliverable *Mapping report on existing EWS*. The primary data source for this document was a standardised questionnaire distributed to all project partners, designed to be completed by, or in coordination with, the competent Civil Protection / Emergency Management authority in each territory.

The questionnaire collected information relevant to governance and decision-making during alerts, including:

- Institutional responsibilities for EWS activation, operation, coordination, and communication;
- The sequence of decision steps across the alert lifecycle (from detection and validation to update and termination);
- Activation of operational coordination structures (e.g., operational rooms, centres, crisis coordination bodies);
- Public warning responsibilities and last-mile arrangements (including authorisation pathways where described).

Partner inputs were complemented, where relevant and available, by official publicly available sources (institutional frameworks, published procedures, and legal/institutional references) to support accurate institutional naming, functional role interpretation, and terminology alignment.

3.3 Consolidation and validation

To ensure consistency and comparability across different national and regional systems, partner inputs were consolidated into a common reporting format (Partner fiches) aligned with the deliverable requirements: analysis of decisional-tree schematisation and main responsibilities in connection to partners' EWS governance arrangements.

The consolidation and validation process followed four steps:

- Completeness screening: verification that minimum governance information was available (decision points, responsible structures, escalation pathways, public warning responsibilities). Where information was incomplete, the relevant fields were marked "Not specified in available sources" to avoid assumptions.
- Terminology harmonisation: mapping local institutional labels and alert-level terminology to a shared set of functional categories (e.g., "technical assessment/issuing body", "operational coordination centre", "local authority/ municipality") to support cross-territory benchmarking.
- Internal consistency checks: verification that descriptions of "who decides" are consistent with descriptions of "who communicates" and "what structures are activated", and that institutions are not assigned mutually exclusive roles unless explicitly described in the collected sources.
- Comparability checks: verification that each fiche contains the same minimum governance elements (decisional tree, activation structures, and responsibilities), so that observed differences across territories reflect governance characteristics rather than reporting format.

Where partner questionnaire responses were received after the initial consolidation cycle, they were processed through the same four-step validation workflow and compiled using the same fiche template to maintain coherence across the full dataset.

3.4 Analysis approach

The analysis is structured around the "chain of command" dimension defined in Activity 1.1 *Mapping and benchmarking of existing EWS, policies and platforms*, with specific attention to the clarity, efficiency, and effectiveness of the command chain during an EWS alert.

Each Partner fiche was compiled using three standard analytical components:

- Decisional tree schematisation: stepwise representation of the alert lifecycle (detection, validation/assessment, classification of alert level, authorisation, dissemination, activation and escalation, updates, termination/stand-down). This directly reflects the scope of this document;
- Activation matrix: concise mapping of which governance and/or operational structures are activated at different alert levels (or phases/colour codes used locally), capturing the transition from routine monitoring to enhanced coordination and emergency command arrangements;
- Key responsibilities (mini-RACI logic): identification of organisations/functions primarily responsible and accountable for a limited set of high-impact decisions (e.g., issuing, upgrading/downgrading alerts, approving public warning messages, activating operational rooms/centres, triggering escalation to higher-level coordination, and terminating the alert).

In addition to mapping, the deliverable flags governance-related gaps and missing elements described in the collected sources (e.g., unclear sign-off procedures, multi-step approval bottlenecks, limited delegation, backup arrangements, fragmented last-mile public warning responsibilities). These observations provide a baseline for follow-up work under *WP1. Benchmarking and assessment of existing Early Warning System (EWS)* focused on weaknesses, gaps, and harmonisation needs.

3.5 Limitations

This deliverable is evidence-based and reflects the information available through partner questionnaire inputs and supporting documentation accessible within the data-collection window. The partnership includes organisations with different institutional mandates; not all project partners are competent authorities mandated to issue EWS alerts. Where a partner's role is primarily support, research, development, or coordination, the mapping captures its interface and support functions within the alert governance chain, rather than attributing an alert-issuing function.

Where information was not available in the collected sources or where a partner reported limited visibility into certain institutional decisions, the relevant elements are reported as "Not specified in available sources". No assumptions were introduced to fill gaps.

Because governance documentation and operational practices may be described at different levels of detail across territories, the mapping prioritises functional comparability over formal equivalence of institutional labels. The document therefore reports decision points and activation structures as described, and uses harmonised functional categories to enable cross-case discussion.

3.6 Quality assurance and comparability

To maximise robustness and usability for subsequent tasks (benchmarking, gap analysis, and recommendations), the following quality assurance principles were applied:

- Evidence-based reporting: only information explicitly provided through partner inputs (including competent authority coordination where applicable) and documented sources was used; assumptions were avoided;
- Uniform minimum dataset: each fiche contains the same minimum governance elements (decisional tree, activation structures, and key responsibilities), enabling structured comparison;
- Traceability: fiche content remains traceable to questionnaire fields, enabling targeted verification and consistent synthesis;
- Separation of concerns: technical system descriptions (platforms, instruments, IT architecture) are addressed primarily in Mapping report on existing EWS, while this document remains focused on decisional governance as required.

4. Reference model “chain of command”

To ensure that governance structures and decision-making pathways are mapped consistently across different national and regional institutional settings, this deliverable applies a single functional reference “chain of command” model. The model does not impose uniform institutional arrangements; instead, it defines a set of governance functions that should be identifiable in every territory, even if functions are merged within one organisation, executed in parallel, or labelled differently. Each Partner Fiche reports the local workflow against this functional logic, so that observed differences can be interpreted as governance characteristics rather than reporting artefacts.

The model is intentionally designed to be compatible with both Italian “allerta” workflows and Croatian alert-management practices, including contexts where emergency communication/dispatch functions (e.g., 112) act as operational coordination touchpoints. The mapping therefore focuses on who performs each governance function and where decision rights sit, rather than on institutional labels alone.

4.1 The unique 6-step flow (functional model)

- Step 1. Detection (signal generation)

Purpose: Identify a potentially relevant hazard signal (forecast, observation, threshold exceedance, field report).

Typical actors (functional): hydro-meteorological or forecasting services, functional centres, monitoring operators, competent technical bodies.

Minimum fiche content (capture): main trigger source(s) (forecast / monitoring / reports), who receives the first signal, and whether triggering is automatic (threshold-based) or expert-driven.

- Step 2. Validation (technical plausibility and data confidence)

Purpose: Confirm reliability of the signal and reconcile conflicting inputs before moving to alert classification.

Typical actors: technical assessment/issuing bodies; in some systems, validation is supported by civil protection duty officers and/or operational monitoring functions.

Minimum fiche content: who validates, any time expectation (if known), and whether validation is formalised (SOP-based) or ad hoc.

- Step 3. Classification (alert level / criticality assignment)

Purpose: Translate validated information into an alert level (criticality) and/or operational phase that triggers predefined preparedness and coordination actions.

Typical actors: technical bodies (often proposing/assigning) and civil protection authorities (sometimes confirming).

Minimum fiche content: local alert levels used (e.g., colours, phases), who assigns/proposes the level, and the main basis (thresholds, expected impacts, expert judgement).

- Step 4. Authorisation (rights to issue, update, escalate/downgrade, terminate)

Purpose: Exercise formal decision rights to issue an alert and determine activation status, including authorisation of updates, upgrades/escalations, downgrades, and termination/stand-down.

Typical actors: competent authority (regional/national civil protection or mandated body); in some systems, co-signature/dual confirmation with technical authorities.

Minimum fiche content: who is accountable for issuing the alert, changing alert level (upgrade/downgrade), and terminating/standing down; whether approval is single-point or multi-step; delegation or backup rules (if available).

- Step 5. Dissemination (institutional notification and public warning interface)

Purpose: Communicate the authorised alert to institutions/responders and the public, or enable decentralised public warning, through official channels.

Typical actors: civil protection operational rooms/centres, emergency communication structures (where applicable), municipalities (often last-mile), authorised spokesperson functions.

Minimum fiche content: institutional dissemination path ("who informs whom"), responsibility and authorisation for public warning content (including updates/cancellation messages where described), last-mile guidance ownership, and channels used (high level).

- Step 6. Activation and escalation (structures, coordination, and alert management over time)

Purpose: Activate the governance/operational structures implied by the alert level and manage escalation and alert evolution over time. This includes activation of coordination structures and resources, escalation to higher command levels when required, and operational alert management (situation monitoring, coordination, and handovers).

Typical actors: operational centres/rooms, coordination bodies (regional/provincial/municipal), responder services, and, where relevant, critical infrastructure operators.

Minimum fiche content: which structures are activated at each alert level (activation matrix), who triggers escalation (vertical/horizontal), how alert evolution is governed over time (e.g., update cadence/authority if known), and who decides/communicates stand-down.

In practice, alerts often evolve through repeated cycles of validation–classification–authorisation–dissemination (Steps 2–5) as new forecasts/observations and impact reports emerge. Step 6 captures how the system is operationally managed during this evolution (coordination, escalation, handovers), while Steps 4–5 capture the governance decision points for changes in alert status and communication.

4.2 What we expect to see in each Partner Fiche (minimum comparable dataset)

To operationalise the model, each Partner Fiche reports the following minimum elements (even if some are "Not specified in available sources"):

- Local alert levels (native terms/colours/phases) and, where possible, mapping to the generic L0–L3 reference scale used in this deliverable.
- Decisional tree aligned to the six steps (compact diagram or stepwise bullets).
- Accountability markers for key decision points, including:
  - who authorises alert issuance, upgrade/downgrade, and termination/stand-down;
  - who authorises public warning content (where applicable);
  - who triggers activation of operational rooms/centres and coordination bodies;
  - who owns last-mile public guidance (often municipal).
- Activation matrix (alert level × activated structures): operational room/centre, coordination body, municipal emergency structure, and high-level responder mobilisation triggers.
- Escalation rules: who escalates to a higher command level, typical triggers, and delegation/backup arrangements (if described).
- Governance control elements: indication of whether SOPs, decision logs/audit trails, and formal documentation exist (Yes / Partial / No / Not specified), without reproducing full documents.
- Public warning message lifecycle governance (where described): who approves and issues initial alerts, updates (including escalation/downgrade), and cancellation/stand-down messages, and how versioning/coherence is ensured between institutional notifications and public-facing communication.

4.3 Notes on comparability and allowed variations

- Merged functions are acceptable (e.g., classification and authorisation within one authority), but the fiche must clearly identify where decision rights sit.
- Different terminology is expected; comparability is achieved through mapping to functional steps and explicit identification of accountable actors.

- Public warning may be decentralised (e.g., municipal last-mile). This is captured as a governance feature and is treated as a gap only where responsibilities/authorisations are unclear or create bottlenecks.
- Operational coordination touchpoints vary: some territories emphasise civil protection operational rooms/centres, while others rely strongly on emergency communication/dispatch functions as coordination nodes. The fiches capture these variations as governance features.
- Where partners cannot provide certain details due to mandate or visibility limits, the fiche reports "Not specified in available sources" rather than inferring responsibilities.

This reference model is applied throughout the deliverable to standardise Partner Fiches and enable structured cross-territory benchmarking of governance and decision-making during EWS alerts.

4.4 Public warning message lifecycle (Alert / Update / Cancel)

Public warning is not a single static product; it is typically managed through a message lifecycle that evolves as forecast confidence, observed conditions, and operational impacts change. For governance mapping purposes, this deliverable distinguishes three functional message types—Alert, Update, and Cancel/Stand-down—and captures, for each partner territory, who is authorised to approve and issue each message type, through which dissemination operators and channels, and how message changes are communicated to institutional recipients and the public.

Alert (initial issuance)

The Alert is the first official message that communicates an expected hazard impact for a defined area and timeframe and initiates predefined readiness, coordination, and response actions. From a governance perspective, the critical element is the authorisation pathway: the competent authority (or co-signature arrangement where applicable) that validates the alert level, approves the content that will be disseminated, and confirms the institutional notification sequence. Partner fiches therefore record: who authorises the initial alert level, who is responsible for drafting and approving public-facing content, and which actors are responsible for last-mile public guidance.

Update (revision, escalation, or downgrade)

The Update is a governance-sensitive message type because it may change preparedness requirements and operational activation status. Updates typically occur due to new forecasts, new observations, impact reports, or changes in confidence/uncertainty. Updates can include escalation (increasing severity), downgrade (decreasing severity), and/or changes to timing, geographic delineation, or recommended actions. For the purposes of this deliverable, an update is treated as a decision point: partner fiches capture who is authorised to approve changes, whether approval is single-point or multi-step, and how updates are communicated to ensure coherence between institutional recipients and public warnings.

Cancel / termination / stand-down (closure)

The Cancel (or termination/stand-down) message formally communicates that the alert is no longer valid or that emergency activation can be reduced or closed. This step is essential for operational clarity and accountability, as it affects deactivation of coordination structures, demobilisation of resources, and return to routine monitoring. Partner fiches therefore record: who has the decision right to terminate/stand down, whether termination is communicated explicitly to institutional recipients and the public, and whether any structured closure practice is referenced (e.g., situation report closure, decision log entry, or after-action review trigger).

Governance relevance for comparability and interoperability

Across partner territories, the same message lifecycle may be implemented with different institutional labels and channels. To support comparability, this deliverable maps message lifecycle governance through functional questions: who authorises each message type, who disseminates it, how last-mile guidance is ensured, and how updates and cancellation are managed to avoid contradictory messages. These elements are particularly relevant for cross-border coordination, as interoperability depends not only on shared situational awareness but also on aligned decision points, consistent versioning of warnings, and clear responsibility for public-facing communication.

5. Governance mapping results overview

5.1 Overview of governance architecture across the Programme Area

The governance mapping confirms that EWS alert management across the Programme Area can be described through a common set of six functional governance steps: detection, validation, classification, authorisation, dissemination, and activation/escalation (including alert updates and stand-down where specified). These functions are identifiable across partner territories, even where they are performed by different institutions, merged within a single organisation, executed in parallel, or described using different administrative terminology.

Across the mapped systems, the governance architecture typically involves a combination of:

- technical bodies responsible for monitoring, forecasting, and technical assessment;
- civil protection and emergency management authorities responsible for authorisation and governance oversight of alert-related decisions and for linking technical assessment to operational activation;
- operational rooms/centres and coordination bodies responsible for managing multi-agency preparedness and response arrangements during alerts;
- municipal authorities responsible for local implementation and last-mile population-facing measures;
- responder organisations (e.g., emergency services) responsible for operational deployment once activated.

Within the Croatian partner territories, the mapping evidences a highly consistent multi-level governance pattern in which national technical warning sources (DHMZ and Croatian Waters) provide hazard warnings that are operationalised through the Civil Protection Directorate and the 112 system. Partner inputs explicitly describe the national 112 Operations Center and the respective Regional 112 Centres as primary joint operational hubs for multi-hazard monitoring and alert coordination, interfacing with County Civil Protection Headquarters and municipal/city civil protection headquarters. In several territories, a County Fire Operations Center (ŽVOC) is described as structured and equipped to function as the County Operational-Communication Center of the County Civil Protection Headquarters (ŽOC CZ), supporting official communications and coordination with competent authorities. Public warning is implemented through a combination of national-level alerting/dissemination mechanisms and local last-mile channels managed by municipal/city authorities and operational services.

Typical governance “handover points” between technical and operational actors occur at: the transition from technical assessment to authorisation (where decision rights are exercised to validate the alert level and activation status); the transition from authorisation to dissemination (where institutional notification and public warning responsibilities are

activated) and the transition from dissemination to activation/escalation (where operational rooms/centres, coordination bodies, and responder mobilisation are triggered). These handovers represent critical points for governance clarity, as they determine who is accountable for decision-making, who ensures coherent messaging and versioning, and which structures take coordination responsibility under time pressure.

Table 1 summarises key actor roles across partner territories by governance function (technical assessment, authorisation, dissemination, public warning interface, operational coordination, and municipal last-mile implementation). It supports quick orientation and cross-territory comparison by presenting “who does what” at a functional level. Entries reflect only partner inputs and documented sources; where information is missing, it is marked “Not specified in available sources” to avoid assumptions.

Table 1 Actor-role overview (by partner/territory)

Territory/Partner	Technical assessment body	Authorisation body	Dissemination operator(s)	Public warning authority	Operational coordination structure	Municipal last-mile role
PP1 – ITALIAMETEO (system-level reference)	Regional functional centres / technical services (system framing)	Not specified in available sources	Civil protection network (high-level)	Mayor / local authority (system framing)	Not specified in available sources	Local implementation under municipal plans (high-level)
PP2 – ARPAE Emilia-Romagna	CF/SGSS (technical assessment as described)	CF + Agency (co-signature, as described)	Official portal + institutional SMS/e-mail (as described)	Mayor (local public-facing interface, as described)	COR (regional coordination hub, as described)	COC/local procedures under municipality (as described)
PP3 – Abruzzo Region (Civil Protection)	Functional Centre (multi-risk monitoring/assessment)	Competent authority by scale (as described)	Dissemination to listed entities (as described) + prefecture interfaces	Public-facing authority not fully specified; local measures via municipal authorities (as described)	Scale-based: COC / CCS / COR / CON (as described)	Municipal activation under civil protection plans (as described)
PP4 – Molise Region	Functional centre (as described)	Regional civil protection service (as described)	PEC/SMS/website via operative chain (as described)	Not specified in available sources	SOR (coordination structure identified)	Municipal implementation (not level-specified in available sources)

PP5 – Marche Region	Functional centre (as described)	Regional civil protection + COR (as described)	PEC/SMS/website via operative chain (as described)	Mayor (local measures/public guidance, as described)	H24 operative room + COR (as described)	Municipal implementation via local plans (as described)
PP6 – Veneto Region	CFD + ARPAV services (technical assessment inputs)	Regional civil protection / governance (as described)	Functional centre/operative chain via PEC/SMS/website (as described)	Mayor (local public warning, as described)	SOR + SSV (coordination/24-7 interface, as described)	Municipal phase adjustment + local guidance (as described)
PP7 – Puglia Region	CFD (technical assessment)	Director (authorises official alert, as described)	Website + PEC/fax + SMS (institutional), municipal channels for public (as described)	Mayor / municipal channels (as described)	SOIR (24/7 coordination, as described)	Municipal last-mile guidance and measures (as described)
PP8 – ZADRA NOVA (Zadar County)	DHMZ + Croatian Waters (national technical sources, as described)	Civil Protection Directorate (112) issues alert instructions (as described); county-level decisions coordinated by County Civil	National 112 system - County Civil Protection HQ + Regional 112 Centre in Zadar; municipal HQ + emergency services (as described)	Local public communication via municipal/city authorities and channels; 112 public alert system also referenced (as described)	National 112 Ops Center + Regional 112 Centre in Zadar; ŽVOC Zadar as County Operational-Communication Center (ŽOC CZ ZZ) (as described)	Municipal/city civil protection HQ + local fire brigades: local alerting, public communication, initial response (as described)

		Protection HQ (as described)				
PP9 – SDC (Split-Dalmatia County)	DHMZ + Croatian Waters (national technical sources, as described)	Civil Protection Directorate (112) issues alert instructions (as described); county-level decisions coordinated by County Civil Protection HQ (as described)	National 112 system - County Civil Protection HQ + Regional 112 Centre in Split; municipal HQ + emergency services (as described)	Public information and last-mile communication via municipal/city channels; 112 public alert system referenced (as described)	National 112 Ops Center + Regional 112 Centre in Split as joint operational hubs; ŽVOC Split as ŽOC CZ SDŽ (as described)	Municipal/city civil protection HQ + local fire brigades: local alerting, public communication, initial response (as described)
PP10 – LIRA (Lika-Senj County)	DHMZ + Croatian Waters (national technical sources, as described)	Civil Protection Directorate / 112 instruction interface (as described)	112 - county/municipal structures + responders (as described)	Local public notice (municipal/county level; not fully specified)	County civil protection structures (as described)	Municipal/city HQ implements measures (as described)
PP11 – Dubrovnik-Neretva County	DHMZ + Croatian Waters (as referenced)	Not specified in available sources	112 / civil protection structures (referenced)	Not specified in available sources	County/local HQ (referenced)	Not specified in available sources
PP12 – Karlovac County Fire	National technical sources (DHMZ/CW) as upstream inputs	Not applicable (responder role)	Operational instructions via 112/civil	Not applicable (responder role)	Responder coordination through HQ	Operational implementation on instruction

Association (VZKZ)			protection chain (as described)		interfaces (as described)	(responder activation)
PP13 – Ruđer Bošković Institute (RBI)	Competent authorities (upstream)	Not applicable (support role)	Official channels (upstream)	Not applicable (support role)	Not applicable (support role)	Support interface (consulted/technical contribution as described)
PP14 – VZIZ (Istria County Fire Association)	DHMZ + Croatian Waters (national technical sources, as described)	Civil Protection Directorate (112) issues alert instructions (as described); county-level decisions coordinated by County Civil Protection HQ (as described)	National 112 system - County Civil Protection HQ + Regional 112 Centre in Pazin; municipal HQ + emergency services (as described)	Local public communication via municipal/city HQ and channels; 112 public alert system also referenced (as described)	National 112 Ops Center + Regional 112 Centre in Pazin; ŽVOC Pula as ŽOC CZ IZ (as described)	Municipal/city civil protection HQ + local fire brigades: local alerting, public communication, immediate protective measures (as described)

5.2 Italy: Mapped governance patterns (partner territories)

Within the Italian partner territories, the mapping indicates a governance pattern in which functional centres and technical assessment bodies play a central role in detection, validation, and classification, while regional civil protection authorities provide authorisation and coordination functions and ensure institutional dissemination through established channels.

Where documented in partner inputs, regional governance includes designated operational rooms and/or coordination structures (e.g., operative rooms, COR/SOR-type bodies) that act as hubs for multi-agency coordination during alert phases. These structures are positioned to coordinate preparedness actions, facilitate information flow between technical bodies and local implementers, and support escalation when events exceed local capacity. In several territories, escalation logic is expressed through a multi-level structure that can move from municipal activation to provincial/prefecture-led coordination (including CCS-type structures where described), and further to regional or national coordination mechanisms depending on severity and scale.

At the municipal level, partner inputs consistently reflect a last-mile governance role for municipal authorities, often with the Mayor as the key public-facing authority for local protective actions and population guidance. Municipal emergency structures (e.g., COC-type centres where described) are activated according to local plans and are connected to the regional chain through institutional notification and coordination interfaces. While regional systems provide structured alert classification and institutional dissemination, public warning and practical guidance to the population may vary depending on local channels and implementation arrangements, which is relevant for comparability and potential harmonisation of public communication interfaces.

5.3 Croatia: mapped governance patterns (partner territories)

Within the Croatian partner territories covered by partner inputs, the governance mapping reflects a multi-level architecture in which national technical warning sources (including hydro-meteorological and water-management bodies, as described) generate warnings that are operationalised through civil protection and emergency communication structures.

A prominent governance feature in the collected sources is the role of the Civil Protection Directorate and the 112 system as the main dissemination and instruction interface linking national-level technical warnings to territorial activation. Partner inputs describe the National 112 Operations Center together with the respective Regional 112 Centres as joint operational hubs for multi-hazard monitoring and alert coordination, interfacing with county civil protection headquarters and municipal/city civil protection headquarters. This interface supports institutional notifications, coordination activation, and the operationalisation of warnings into territorial preparedness and response actions.

County-level civil protection headquarters and local (municipal/city) headquarters are described as key operationalisation structures responsible for translating warnings into local readiness measures and coordinated actions. In several territories, partner inputs also describe the County Fire Operations Center (ŽVOC) as structured and equipped to function as the County Operational-Communication Center of the County Civil Protection Headquarters (ŽOC CZ), supporting official communications, multi-agency coordination, and operational continuity during alert situations.

Responder activation is reflected through the mobilisation of operational services (including firefighting organisations where documented), which act as response arms once alerts and/or operational instructions trigger deployment, readiness, or protective measures.

Public warning governance in the mapped Croatian inputs is described primarily through the combination of nationally issued warnings and territorial dissemination/implementation responsibilities. Where detailed specification of public-facing authorisation pathways (e.g., sign-off for public-facing text, update/cancellation message approvals, or channel-by-level rules) is not available in the collected sources, the mapping records the institutional actors involved and the operationalisation logic without inferring message approval procedures. This enables functional comparison with Italian partner territories by documenting decision points and activation structures while respecting differences in institutional terminology and mandate distribution.

The purpose of Table 2 is to support comparability across different institutional terminologies (Italy–Croatia and across regions) by providing a practical “term-to-function” bridge. The catalogue does not harmonise legal definitions or mandates; it reports how structures are described in available sources and how they are mapped to the reference chain-of-command steps. Where a structure is not mentioned in partner inputs, this is not interpreted as absence; it is treated as not specified in available sources.

Table 2. Activation structures mentioned in partner inputs (catalogue)

Structure / term (as referenced)	Functional meaning (in this deliverable)	Referenced in partner fiches (examples)	Notes on use in mapping
Functional Centre / CFD / CF / technical assessment body	Technical assessment, validation and/or alert classification	PP2, PP3, PP4, PP5, PP6, PP7	May also co-sign or propose levels depending on territory
DHMZ / Croatian Waters (national technical warning sources)	**Upstream technical warning / monitoring and hazard assessment inputs (Croatia)**	**PP8, PP9, PP10, PP11, PP14 (and responder/support partners where referenced)**	Captured under Detection/ Validation/Classification as upstream technical sources
Civil Protection Directorate (Croatia)	**Competent civil protection governance interface for operationalisation of warnings and coordination activation**	**PP8, PP9, PP10, PP11, PP14 (as described)**	Captured across Authorisation/ Dissemination/Activation steps depending on sources
National 112 Operations Center (Croatia)	**National-level operational hub supporting multi-hazard coordination, dissemination, and instruction interfaces**	**PP8, PP9, PP14 (as described)**	Captured under Dissemination and Activation/Escalation as a governance touchpoint
Regional 112 Centre (Croatia)	**Regional operational hub for dissemination, coordination activation, and multi-agency interface**	**PP8, PP9, PP14 (as described)**	Captured as a key operational node linking national warnings to county/municipal structures
County Fire Operations Center (ŽVOC) / County Operational-Communication Center of County Civil Protection HQ (ŽOC CZ)	**County-level operational-communication and coordination hub (Croatia), supporting official communications and continuity**	**PP8, PP9, PP14 (as described)**	Mapped under Activation/Escalation; treated as an operational coordination structure where explicitly described

Operative room / SOR / regional operations room	Operational coordination and institutional dissemination hub	PP4, PP5, PP6	Role and naming vary; mapped functionally as coordination node
COR (regional coordination body / crisis unit)	Multi-agency coordination structure activated during alert phases	PP2, PP5, PP6	Activation triggers may be qualitative in sources
SOIR (Puglia)	Regional operational coordination structure (24/7)	PP7	Treated as coordination hub for activation/escalation
SSV (Veneto)	24/7 contact/interface supporting coordination	PP6	Mapped as operational interface function
COC (municipal operations centre)	Municipal coordination structure for local preparedness/response	PP2 (as described), PP3, PP6, PP7	Municipal activation often depends on local plans
CCS (prefecture-led coordination)	Provincial-level rescue coordination (Italy)	PP2, PP3, PP7 (as described)	Appears as escalation structure for severe events
Prefecture / UTG (Italy)	Provincial authority role in coordination/escalation and convening CCS	PP2, PP3, PP7	Captured as escalation/coordination function
CON (national coordination committee)	National-level coordination structure for large-scale events	PP3	Included where scale-based governance is described
County civil protection HQ / local HQ (Croatia)	County/municipal operationalisation and coordination	PP8, PP9, PP10, PP11, PP14	Used for activation/escalation mapping
Responder organisations (e.g., fire brigades/associations)	Operational deployment once activated/instructed	PP8, PP9, PP10, PP12, PP14	Captured as implementation/activation node (responder role where applicable)

5.4 Cross-cutting comparison and interoperability-relevant touchpoints

Across the Programme Area, the mapping demonstrates that differences in EWS governance are less about the existence of core functions and more about how decision rights and operational responsibilities are distributed across levels and how handovers are formalised. Comparative interpretation is therefore based on functional decision points rather than forced equivalence of institutional labels.

A first cross-cutting lens concerns decision rights distribution. Some mapped arrangements emphasise decentralised implementation with strong municipal roles in last-mile measures and public-facing guidance, while others rely on centralised dissemination and instruction interfaces that guide territorial activation. A second lens concerns escalation points: escalation is typically triggered by increasing severity, forecast uncertainty, or operational need, but the degree to which escalation rules are formalised and the bodies responsible for convening coordination structures vary across territories.

A third lens concerns the public warning interface, including who approves public-facing content and who owns last-mile guidance. In many mapped settings, municipal authorities are central to last-mile communication and implementation, while regional or national structures ensure institutional dissemination and coordination. From an interoperability perspective, clarity on who can approve and issue public warning messages—including updates and cancellation/stand-down messages—is critical to avoid contradictory messaging and to ensure coherent communication across boundaries and jurisdictions.

A fourth lens concerns update/stand-down governance. The message lifecycle (Alert/Update/Cancel/Stand-down) represents a decision chain over time, and the mapping records whether the authority and procedure for updates and termination are explicitly specified. Where these elements are not detailed in the collected sources, they are reported as not specified, as they represent governance touchpoints that can affect operational clarity, accountability, and the consistency of institutional and public-facing communications.

A fifth lens concerns traceability and governance controls, including whether SOPs, formal procedures, or decision logging/audit trail elements are referenced. Such controls support accountability and after-action learning and can strengthen cross-border cooperation by clarifying how decisions are documented, versioned, and communicated.

Finally, the mapping identifies interoperability-relevant governance touchpoints likely to matter for cross-border coordination, including: information-sharing interfaces between technical and operational bodies, synchronisation and versioning of warning updates, and the alignment of roles and handovers between institutional notifications and public messages.

5.5 Summary of recurring strengths and recurring ambiguities

Based on the partner fiches, several recurring strengths are observed across multiple territories. These include the presence of a clear multi-level governance chain; the existence of designated coordination structures (operational rooms/centres and coordination bodies where described); and an established role for municipal authorities in last-mile implementation and public guidance. In a number of cases, the mapping also indicates structured institutional dissemination mechanisms and operational coordination interfaces that support rapid escalation and multi-agency mobilisation when severity increases. In the Croatian partner territories, partner inputs frequently document a consistent operationalisation pathway from national technical warnings to territorial activation through the 112/civil protection interface and associated operational hubs.

At the same time, the mapping identifies recurring ambiguities and potential bottlenecks in available sources that are relevant as a baseline for WP1.2 work. These include: incomplete specification of update/stand-down decision rights (who authorises termination and how it is communicated); limited clarity on message approval chains (especially for public-facing text and for updated/cancellation messages); incomplete or non-uniform activation-by-level matrices; and limited detail on substitution/delegation arrangements for key authorising roles. These issues are governance-relevant not because they indicate system failure, but because they can reduce clarity under time pressure and create friction points for harmonisation and interoperability.

6. Partner / Regional fiches (benchmarking format)

How to read these fiches

Each Partner fiche follows the same structure (A–F) and applies the reference 6-step flow (detection → validation → classification → authorisation → dissemination → activation/escalation). The fiches report only information supported by partner inputs and documented sources. Where information was not available, it is stated as "Not specified in available sources" to avoid assumptions.

This chapter reflects all partner inputs available at the time of compilation; questionnaires received after the initial consolidation cycle were integrated using the same fiche template and validation rules to preserve comparability and traceability.

Partners have different mandates within the EWS ecosystem. Some partners operate as competent authorities within the alert chain (issuer/coordinator), while others contribute through responder or support/competence-centre roles. Where a partner is not mandated to issue alerts, the fiche records the partner's position and interfaces in the governance chain without attributing alert-issuing authority.

Fiche typology and benchmarking applicability

To enable consistent interpretation and meaningful comparison across territories, fiches are grouped into functional types reflecting each partner's position in the alert governance chain:

Type A – Issuer/Coordinator fiche (benchmarkable, level-by-level where possible)

Type A fiches describe territories and institutions that have a direct role in issuing, authorising, and/or coordinating EWS alerts and related operational activation. In the Croatian context, alerts are typically based on nationally issued technical warnings (e.g., DHMZ and Croatian Waters) and operationalised through the Civil Protection Directorate/112 and county/local civil protection structures; therefore, Type A fiches may capture county-level coordination and operationalisation roles even where the partner institution is not the technical warning issuer. These fiches typically provide sufficient detail to support level-by-level benchmarking, including local alert-level taxonomy (e.g., colour codes/phases), activation matrices, and accountability for key decisions (issuance, escalation/downgrade, updates, termination/stand-down, activation of coordination structures, and public warning interfaces). Type A fiches form the primary basis for comparative matrices in this deliverable.

Type B – Responder fiche (benchmarking of activation/escalation and operational decision points)

Type B fiches represent partners whose role is primarily operational response (e.g., emergency services and responder organisations) and who are recipients of alerts and instructions rather than competent authorities for alert issuance. These fiches provide

evidence on how alerts are operationalised in practice, including activation triggers, escalation pathways, coordination interfaces, and decision points related to mobilisation, field operations, and reporting back to coordination structures. Type B fiches are used to map activation/escalation interfaces relevant for interoperability.

Type C – Support / competence-centre fiche (benchmarking of interfaces and support governance)

Type C fiches cover partners that do not issue alerts and are not response command structures but provide technical, scientific, data, analytical, or coordination support to competent authorities and responders. These fiches map governance arrangements for expert support (consultation triggers, data-sharing practices, interface points during time-critical situations). Type C fiches strengthen the understanding of how decision-makers access and use technical inputs and where formalisation of support mechanisms may improve readiness and interoperability.

Reference fiches (system framing; not benchmarked level-by-level)

Where a partner provides system-level framing rather than a territory-specific governance description, the fiche is retained as a reference/terminology bridge. Such fiches are not used for level-by-level benchmarking because their respondent nature and data granularity differ from territorial Type A fiches.

Use of fiche types in this deliverable

All fiche types are included to represent the full governance network within the Programme Area. However, comparative benchmarking of alert-level governance relies primarily on Type A fiches where sufficient information is available. Type B and Type C fiches complement the mapping by documenting activation pathways and support interfaces, without attributing alert-issuing authority where it is not mandated.

6.1 National Agency for Meteorology and Climatology- ITALIAMETEO (PP1 – Italy)

A) Role in the EWS chain

Reference fiche (system framing; not benchmarked level-by-level)

Provides high-level framing of Italian EWS governance as a decentralised but coordinated system: at national level the National Civil Protection Department (DPC) sets strategic policy and oversees the system; at regional level Regional Functional Centres (CFRs) manage operational EWS activities and issue region-specific alert bulletins; at local level the Mayor acts as local Civil Protection Authority responsible for activating local plans and communicating protective actions to the public. A national 24/7 coordination/monitoring function is referenced through the DPC National Operational Centre (S.O.N.).

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Functional scheme

- Detection: monitoring and modelling within national/regional technical services (high-level).
- Validation: performed within regional functional/technical structures (CFRs) (high-level).
- Classification: CFRs issue graded alert bulletins based on forecasts and predefined thresholds (high-level).
- Authorisation: tiered decision-making for protective actions, with key protective-action decisions at local level (Mayor); Prefecture referenced as relevant for coordination depending on event scale.
- Dissemination: via the Civil Protection network (high-level); public-facing channels not specified in available sources.
- Activation/escalation: activation of local plans and actions under municipal emergency planning; national coordination role referenced for large/multi-hazard events (high-level).

Interpretation notes:

- System-level framing only; not a territory-specific workflow.
- Several questionnaire fields are incomplete (e.g., detailed chain-of-command steps and public channels), therefore not benchmarked as a Type A territorial fiche.
- Use as terminology bridge and contextual framing; do not compare level-by-level with territorial fiches.

C) Activation matrix (alert level × activated structures)

Note	Value
Territorial activation matrix	Not applicable (system-level reference); no level-by-level activation mapping provided

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Benchmarking status	Not applicable for	-	-	-

	benchmarking (reference only).			

E) Bottlenecks / unclear points

- Detailed chain-of-command from detection to dissemination not specified in available sources.
- Public warning channels and alert-level governance not specified.
- No activation-by-level matrix.

F) Data note

Included as system framing/reference; not used for quantitative or level-by-level benchmarking.

6.2 Regional Agency for Prevention, Environment and Energy in Emilia Romagna (PP2 – Italy)

A) Role in the EWS chain

Type A – Issuer/Coordinator

Technical assessment and classification are performed through the ARPAE–SIMC Functional Centre (CF) together with SGSS, with collaborative multi-hazard evaluation. Official regional bulletins (Allerta / Monitoring Bulletin) are issued under a joint signature (co-signature) arrangement (CF + Regional Agency for Territorial Safety and Civil Protection, as described). COR operates as the regional coordination hub during alert phases. Municipalities (Mayor/COC) implement local measures and provide public-facing guidance.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: CF + SGSS forecasting/monitoring inputs; additional streams include avalanche technical assessment (Meteomont bulletin by Regional Carabinieri Forestry Command) integrated for colour-code assignment (as described).
- Validation: CF/SGSS technical verification and integrated evaluation (as described).
- Classification: graded colour-code levels green/yellow/orange/red (as described).
- Authorisation: issuance formalised via Allerta meteo idrogeologica idraulica / Bollettino di vigilanza under double signature (CF + Agency) (as described).

- Dissemination: publication via the official regional alert portal plus institutional notifications (SMS/e-mail) to recipients (Municipalities, Prefectures, and other operational structures) for Yellow+ (as described).
- Activation/escalation: COR as regional coordination hub; for severe cases Prefecture/UTG may convene CCS; municipalities activate local procedures (COC) and Mayor communicates self-protection measures (as described). During events (notably river floods), CF may maintain H24 presidium and issue monitoring documents (as described).

C) Activation matrix (alert level × activated structures)

Alert level	CF (forecast/monitor)	COR / regional ops	Prefecture/CCS	Municipality/COC	Specialised flood actors
Green / Monitoring bulletin	Yes	No	No	No	No
Yellow	Yes	As needed	No	Local plan checks	As needed
Orange	Yes (H24 possible)	Yes	Possible CCS	Yes (if needed)	Yes
Red	Yes (H24)	Yes	Likely CCS	Yes	Yes

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Validate forecast/monitoring data	CF/SGSS	CF	Agency	COR, municipalities
Set colour-code criticality	CF/SGSS (+ avalanche input where relevant)	CF + Agency	SGSS, relevant technical bodies	Prefectures, municipalities
Issue official alert bulletin	CF	CF + Agency (co-sign)	SGSS	All recipients
Institutional dissemination (SMS/e-mail/web)	CF/Agency	Agency	COR	Recipients

Activate/scale COR (incl. H24)	Agency/COR	Agency	CF	Prefectures, municipalities
Convene CCS (provincial)	Prefecture	Prefecture	COR/Agency	Municipalities
Open COC + local measures	Municipality	Mayor	COR/Prefecture	Population
Public warning/self-protection info	Municipality	Mayor	COR	Population

E) Bottlenecks / unclear points

- Time targets/SLAs per step not quantified.
- Substitution rules for key signatories not described.
- CCS/COC activation triggers described qualitatively.

F) Data note

Not specified in available sources: explicit timings/SLAs, fallback authorisation rules, fully quantified escalation thresholds.

6.3 Regional Civil Protection Agency – Abruzzo Region (PP3- Italy)

A) Role in the EWS chain

Type A – Issuer/Coordinator (scale-based governance).

The Abruzzo Functional Centre is responsible for multi-risk monitoring and alerting. Emergency management and coordination are described as scale-dependent, with activation of COC/CCS/COR/CON depending on territorial scale. Ordinance powers for urgent measures are referenced across multiple levels (Mayor/Regional President/Prefect/Prime Minister, as described).

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: Abruzzo Functional Centre (multi-risk monitoring).
- Validation: Abruzzo Functional Centre (as described).

- Classification: warning levels defined through a colour-scale green/yellow/orange/red (as described) and issued through the regional multi-risk alerting system; operational continuity relies on on-call coverage supported by other departments (as described).
- Authorisation: issuance performed within the regional alerting system; competent authority/urgent measures depend on event scale (as described). SOPs are referenced as contained in the Regional Multi-Risk Alerting System approved by Decree of the President of the Region (as described).
- Dissemination: after issuance, each recipient follows procedures in its civil protection plan; Prefectures, under agreement with the Functional Centre, alert Fire Brigade and law enforcement (as described). Dispatch through an alerting platform is referenced (as described).
- Activation/escalation: scale-driven activation of operational task-force/coordination centres: COC (municipal), CCS (provincial; convened by Prefect), COR (multi-province/regional), CON (national large-scale) (as described).

C) Activation matrix (alert level × activated structures)

Because governance is reported primarily by scale rather than by explicit "structures per colour level", activation is mapped as follows:

Alert/emergency scale	Activated structures
Municipal event	COC (Municipal Operations Centre)
Provincial event	CCS (Prefect-led Rescue Coordination Committee)
Multi-province event	COR (Regional Operations Committee)
National large-scale	CON (National Operations Committee)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Multi-risk monitoring & technical warning	Functional Centre	Functional Centre	Not specified	Recipients
Issue/dispatch alert message	Functional Centre (on-call)	Functional Centre /	IT/admin support (dispatch	Listed recipients

(platform-supported)		regional system	support, as described)	
Prefecture alerts Fire Brigade & law enforcement	Prefecture	Prefecture	Functional Centre (agreement)	Municipalities/actors
Convene CCS (provincial)	Prefecture	Prefecture	Functional Centre, responders	Municipalities
Activate COR/CON (regional/national)	Region / national authority	Region / national authority	Prefectures, responders	All actors
Local protective measures / ordinances	Municipality/Prefecture/Region (as applicable)	Respective authority	Responders	Public

E) Bottlenecks / unclear points

- Detailed public warning channels and message approval chain for public-facing text are not specified.
- Time targets between issuance and activation of structures not stated.
- Update/stand-down authorisation and cancellation messaging not detailed.

F) Data note

Strong evidence on scale-based escalation structures (COC/CCS/COR/CON) and Prefecture interface. Not specified: detailed public warning governance, update/stand-down procedures, quantified timing targets.

6.4 Molise Region (PP4- Italy)

A) Role in the EWS chain

Type A – Coordinator (regional civil protection service + SOR).

Technical assessment and bulletin dissemination are attributed to the Regional Functional Centre (as part of the national functional centre network). Regional civil protection service

manages governance decision-making and operational coordination, with SOR (Regional Operational Room) identified as the coordination and management structure for regional emergency situations (as described; formally established by regional law n.10/2000, art.13).

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: Regional Functional Centre (as described).
- Validation: Regional Functional Centre (as described).
- Classification: warning levels follow the national homogenised approach and are described through a colour-scale green/yellow/orange/red (national model referenced; local detailed thresholds not specified).
- Authorisation: regional civil protection service (with internal components; multi-institutional representation referenced broadly) (as described).
- Dissemination: Functional Centre - Regional Civil Protection Operative Room - dissemination to civil protection system actors and municipalities via PEC, SMS, website (as described).
- Activation/escalation: SOR coordinates and manages regional emergencies; detailed escalation triggers (e.g., CCS/COC thresholds) not specified in available sources. Framework agreements for regional emergency management are reported as under consultation; until finalised, national rules apply (as described). SOPs referenced (DGR 78/2018).

C) Activation matrix (alert level × activated structures)

Alert level	Functional Centre	SOR	Municipalities/COC	Prefecture/CCS
Green	Yes	Not specified	Not specified	Not specified
Yellow/Orange/Red	Yes	As needed (not specified by level)	As needed (not specified by level)	As needed (not specified by level)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Technical assessment & bulletin preparation	Functional Centre	Functional Centre	Regional CP service	SOR, municipalities
Institutional dissemination to actors/municipalities	Regional CP Operative Room	Regional CP service	SOR	Municipalities/actors
Regional emergency coordination	SOR	Regional CP service	Represented institutions	Municipalities/actors

E) Bottlenecks / unclear points

- Activation-by-level matrix not detailed (limits benchmarking comparability).
- Role of Prefecture/CCS and municipal COC activation rules not described in detail.
- Public warning authorisation and message approval chain not specified.

F) Data note

Solid evidence on standard dissemination chain (PEC/SMS/website), SOR role, and existence of SOP reference (DGR 78/2018). Not specified: level-by-level activation triggers, escalation thresholds, and public warning governance details.

6.5 Marche Region (PP5- Italy)

A) Role in the EWS chain

Type A – Coordinator (regional civil protection + COR) with H24 operative room.

The Regional Department of Civil Protection and COR (Regional Operations Committee and Crisis Unit) provide coordination and decision-making during alerts, with multi-institutional representation (as described). A regional civil protection operative room is reported as operative H24 (as described). The Regional Functional Centre is responsible for alert bulletin dissemination as part of the national functional centre network.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: Regional Functional Centre (as described).
- Validation: Regional Functional Centre (as described).
- Classification: warning levels follow a colour-scale green/yellow/orange/red (national homogenised model referenced; detailed thresholds not specified).
- Authorisation: regional Marche civil protection department together with COR (as described, governance/coordination).
- Dissemination: Functional Centre - Regional Civil Protection operative room - dissemination to regional civil protection system actors and municipalities via PEC, SMS, website (as described).
- Activation/escalation: COR coordinates and manages regional emergency situations; H24 operative room supports continuous operations. Municipalities implement measures under local plans. Procedures/SOPs are explicitly referenced (DPGR 84/2023; DPGR 160/2016; DPGR 63/2017; DGR Marche 148/2018), including correlation between broadcast alert and operative actions (as described).

C) Activation matrix (alert level × activated structures)

Alert level	Functional Centre	Operative room	COR	Municipalities/COC
Green	Yes	Not specified	Not specified	Not specified
Yellow/Orange/Red	Yes	Yes (H24)	Yes (coordination)	Yes (via local plans)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Disseminate alert to municipalities/system actors	Operative room	Regional CP	COR	Municipalities/actors
Coordinate regional emergency management	COR	Regional CP	Represented institutions	Municipalities/actors

Local protective measures & public guidance	Municipality	Mayor	COR / Prefecture (where relevant)	Public

E) Bottlenecks / unclear points

- Detailed activation-by-level thresholds (e.g., when COC/CCS become mandatory) not specified.
- Public warning message approval chain (who signs public-facing text) not specified.
- Update/stand-down decision rights not detailed.

F) Data note

Strong evidence on COR + H24 operative room and dissemination channels; explicit SOP references support traceability. Not specified: quantified thresholds and detailed governance for public message approval and stand-down.

6.6 Veneto Region (PP6- Italy)

A) Role in the EWS chain

Type A – Coordinator and institutional dissemination actor (regional civil protection + COR), with SOR/SSV operational interfaces.

Functional Centre (CFD) and ARPAV services provide technical monitoring/assessment; the region coordinates governance decisions and dissemination through the operative chain. SOR coordinates and manages emergencies at regional level; SSV (Sala Situazioni Veneto) provides a 24/7 contact interface (green number) (as described). Municipalities may autonomously activate/adjust local operational phases; Mayor communicates local measures and self-protection guidance (as described).

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: CFD + ARPAV services (monitoring/inputs).
- Validation: CFD (as described).
- Classification: four-level scheme green/yellow/orange/red aligned with national scenario tables (as described).
- Authorisation: regional civil protection governance + COR (regional operations committee/crisis unit) (as described).

- Dissemination: Functional Centre - Regional Civil Protection operative room (SOR chain) - municipalities/actors via PEC, SMS, website (as described).
- Activation/escalation: SOR coordinates regional emergencies; SSV provides 24/7 interface. Local authorities (Mayor) may adjust operational phase based on local situation and communicate measures to the population using methods defined in local plans. SOPs/acts are extensively referenced (list provided in questionnaire).

C) Activation matrix (alert level × activated structures)

Alert level	CFD	SOR / SSV	COR	Municipality/COC
Green	Yes	Not specified	Not specified	Not specified
Yellow	Yes	Yes	As needed	Yes (local plan)
Orange	Yes	Yes	Yes	Yes
Red	Yes	Yes	Yes	Yes

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Validate monitoring/forecast data	CFD/ARPAV	CFD	Competence centres (where relevant)	Regional CP
Set/confirm alert level	CFD (technical)	Regional CP (governance)	COR	Municipalities
Disseminate institutional warning	SOR (operative chain)	Regional CP	COR	Municipalities/actors
Coordinate regional response	SOR	Regional CP	COR	Municipalities/actors
Adjust local operational phase	Municipality	Mayor	Region/SOR	Public

Local public guidance & measures	Municipality	Mayor	SOR	Public
Stand-down / deactivation	Region + Municipality (as described generally)	Region / Mayor	COR	All actors

E) Bottlenecks / unclear points

- Municipal variability in public-warning channels can reduce uniformity/interoperability.
- SMS public-warning procedure is under testing (maturity varies).
- COR activation thresholds not fully quantified.

F) Data note

High comparability: explicit alert levels and clear operative-chain dissemination; strong description of local phase adjustment logic. Minor clarifications would require more detail on formal COR triggers and update/termination governance.

6.7 Puglia Region (PP7- Italy)

A) Role in the EWS chain

Type A – Issuer/Coordinator (CFD + Director authorisation; SOIR/COR coordination; municipal last-mile).

National forecasts are received from the national level and validated/analysed by the regional Decentralised Functional Centre (CFD). CFD produces bulletins and proposes criticality; the Director of the Civil Protection Section authorises the issuance of the Official Alert Message (as described). SOIR (within the regional operations/correlation framework) coordinates emergency management 24/7 and liaises with Prefectures (CCS) and Municipal Operations Centres (COC). Municipalities implement local plans and communicate to the public via local channels.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: national meteorological forecasts + regional monitoring network real-time data (as described).
- Validation: CFD validates national forecasts and integrates regional data (as described).
- Classification: CFD correlates forecast values with thresholds and assesses impacts by Alert Zone; criticality classes (Ordinary/Moderate/Elevated) correspond to Yellow/Orange/Red alert levels (as described). The alert message includes zone-based alert level and recommended operational phase (Attention / Pre-Alert / Alert) (as described).
- Authorisation: Director reviews CFD assessments and authorises the issuance of the Official Alert Message (as described).
- Dissemination: Official Alert Message published on regional civil protection/CFD website and sent to designated recipients (Prefectures, Municipalities, regional operational structures, service/network operators) via PEC or fax, with SMS notifications to authorities/stakeholders for rapid dissemination (as described).
- Activation/escalation: SOIR coordinates response 24/7; CCS and COC are activated for Yellow/Orange/Red (as described). Municipalities activate local resources and disseminate warnings to the public via apps, sirens, social media, and additional channels (including door-to-door if needed, as described). Ongoing monitoring and updates are provided throughout events (update/termination governance not detailed).

C) Activation matrix (alert level × activated structures)

Alert level	CFD	SOIR (coordination)	Prefecture/CCS	Municipality/COC
Yellow	Yes	Yes	Yes	Yes
Orange	Yes	Yes	Yes	Yes
Red	Yes	Yes (24/7)	Yes	Yes

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Validate forecasts vs thresholds	CFD	CFD	National inputs	SOIR

Set criticality / alert level (by zone)	CFD	Director (authorisation)	SOIR	Prefectures/municipalities
Approve official alert message	CFD (draft)	Director	SOIR	Recipients
Institutional dissemination (PEC/fax/SMS/website)	CFD/SOIR	Regional CP (Director)	Prefectures	Municipalities/actors
Operational coordination during alert	SOIR	Regional CP	CCS/COC	Responders/actors
Last-mile public warning	Municipality	Mayor	SOIR	Public

E) Bottlenecks / unclear points

- Channel-by-level mandatory rules are not fully specified (which channel is compulsory at which alert level).
- Update and termination/stand-down authorisation and "all-clear" messaging are not explicitly mapped.
- Trigger for enhanced duty patterns (beyond "critical events") not quantified.

F) Data note

Very good benchmarking value on authorisation (Director) + zone/phases + multi-channel dissemination and SOIR 24/7 role. Not specified: detailed termination governance and formal channel-by-level rules.

6.8 Zadar County Development Agency ZADRA NOVA (PP8 - Croatia)

A) Role in the EWS chain

Type A – Coordinator (county-level operationalisation of nationally issued warnings).

Zadar County operates within Croatia's national multi-hazard EWS. The governance chain is characterised by national technical warning sources (DHMZ; Croatian Waters) and a

centralised civil-protection dissemination/coordination interface (Civil Protection Directorate through the 112 system). At county level, the Zadar County Civil Protection Headquarters coordinates regional actions and distributes warnings to municipalities; municipal civil protection headquarters execute last-mile preparedness and response. The County Fire Operations Center (ŽVOC Zadar) is structured and equipped to function as the county Operational-Communication Centre of the County Civil Protection HQ (ŽOC CZ ZZ) for official communications and operational continuity

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: hazard signals generated through national monitoring/forecasting networks (meteorological and hydrological monitoring).
- Validation: technical plausibility/verification performed by competent technical bodies (DHMZ; Croatian Waters), supported by their IT platforms/models.
- Classification: warning levels communicated using DHMZ colour-coded warnings (yellow/orange/red) and Croatian Waters flood alert phases (regular/emergency flood defence levels).
- Authorisation: national civil protection governance/activation described as led by the Civil Protection Directorate (Ministry of the Interior) through the 112 system; county-level operational decisions are coordinated through county and municipal civil protection structures.
- Dissemination: multi-hazard monitoring and alert coordination routed through the national 112 Operations Center and Regional 112 Centre in Zadar, interfacing with the County Civil Protection HQ and municipal authorities; public warning includes 112 public alerting and local municipal channels.
- Activation/escalation: county and local structures operationalise warnings into preparedness/response actions; ŽVOC Zadar supports official communications as ŽOC CZ ZZ; emergency services (fire brigades, police, medical) provide field response.

Data completeness note: specific approval/sign-off steps for public-facing message text (alert/update/cancel) and update/stand-down decision rights are not specified in available sources.

C) Activation matrix (alert level × activated structures)

Level-by-level activation thresholds are not specified in available sources; activation is described as instruction- and plan-based within the national system.

Warning reference in partner input	National 112 / CP Directorate interface	Regional 112 Centre (Zadar)	County CP HQ	ŽVOC / ŽOC CZ ZZ	Municipal CP HQ + responders
DHMZ colour-coded warnings (yellow/orange/red); Croatian Waters flood phases	Yes (national alert activation/coordination interface)	Yes (primary joint operational hub)	Yes (county coordination/distribution)	As needed (official comms/continuity support)	Yes (local alerting, readiness, response)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Issue meteo/hydro warnings and classify level	DHMZ / Croatian Waters	DHMZ / Croatian Waters	CP Directorate (112)	County/municipal structures
Activate national alert coordination / route operational messages	CP Directorate / 112 system	CP Directorate	DHMZ/CW	County CP HQ, municipalities, responders
County-level coordination and distribution to municipalities	County CP HQ	County CP HQ	Regional 112 Centre; ŽVOC/ŽOC (as needed)	Municipal HQ, responders
Operational-communication continuity (ŽOC CZ ZZ function)	ŽVOC Zadar	County CP HQ	Regional 112 Centre	Relevant authorities/actors

Last-mile public communication and local protective measures	Municipal authorities / municipal CP HQ	Municipal leadership (not specified)	County CP HQ	Public

Roles are recorded functionally; specific named signatories for public text approval are not specified in available sources.

E) Bottlenecks / unclear points

- No county-owned independent multi-hazard centre; coordination is integrated into the national 112 system (governance feature; implies reliance on national nodes).
- Public warning message approval chain (who approves/versions public text for alert/update/cancel) is not specified.
- Update/termination (stand-down) decision rights and procedures are not explicitly mapped.

F) Data note

The fiche is supported by partner input describing: legally responsible institutions and division of responsibilities; national warning level schemes and dissemination channels; the national 112 + Regional 112 operational hub model and ŽVOC's ŽOC function; and (iv) existence of SOPs and contingency plans at national and local levels (County CP Plan, County Risk Assessment, Municipal CP Plans; Fire Protection Plan).

6.9 Split-Dalmatia County (PP9- Croatia)

A) Role in the EWS chain

Type A – Coordinator (county-level operationalisation of nationally issued warnings).

Split-Dalmatia County operates within Croatia's national multi-hazard EWS with national technical warning sources (DHMZ; Croatian Waters; additionally listed national seismic and wildfire monitoring bodies) and a centralised civil-protection dissemination/coordination interface via the Civil Protection Directorate / 112 system. At county level, the Split-Dalmatia County Civil Protection Headquarters coordinates regional actions and distributes warnings to municipalities; municipal civil protection HQs conduct local alerting, readiness, and response. Firefighting associations and the County Fire Operations Center (ŽVOC) are responsible for alerting and coordinating firefighting units.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: national multi-hazard monitoring networks (meteorological; hydrological; plus hazard monitoring bodies listed in the input for earthquakes and wildfires).
- Validation: technical verification performed by competent national bodies using their IT systems/models (e.g., DHMZ platforms; HIROS/Croatian Waters databases).
- Classification: warning levels communicated through DHMZ colour-coded system (yellow/orange/red) and Croatian Waters flood alert phases; operational messages distributed to county/local authorities via the civil protection/112 interface.
- Authorisation: national alert activation/coordination led by the Civil Protection Directorate through the 112 system; county-level decisions coordinated by county civil protection headquarters (as described).
- Dissemination: national 112 system routes warnings/operational messages to county and municipal structures; public warning uses 112 public alerts plus local channels (municipal websites/social media, media broadcasts, sirens in selected municipalities, phone/telephone notifications as listed).
- Activation/escalation: county and municipal civil protection HQs operationalise warnings into readiness/response; responders (incl. firefighting units coordinated through ŽVOC) provide field implementation.

Data completeness note: update/stand-down authority and public-message sign-off/versioning are not specified in available sources.

C) Activation matrix (alert level × activated structures)

Level-by-level activation thresholds are not specified in available sources; the input confirms warning level taxonomies and the multi-level dissemination/implementation chain.

Warning reference in partner input	National 112 / CP Directorate interface	County CP HQ	ŽVOC / firefighting coordination	Municipal CP HQ + responders	Public warning channels
DHMZ (yellow/orange/red) + Croatian	Yes	Yes	As needed (firefighting	Yes	112 public alerts + municipal

Waters flood phases			activation/coordination)		channels/media/sirens (as listed)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Issue meteo/hydro warnings and classify level	DHMZ / Croatian Waters	DHMZ / Croatian Waters	CP Directorate / 112	County/municipal structures
Route operational messages and activate national alert coordination	CP Directorate / 112 system	CP Directorate	DHMZ/CW	County CP HQ, municipalities, responders
County distribution/coordination to municipalities	County CP HQ	County CP HQ	Regional CP Office / 112 interfaces (as applicable); firefighting coordination bodies	Municipal HQ, responders
Coordinate firefighting units under alert/operations	Firefighting Associations / ŽVOC	County firefighting coordination (as described)	County CP HQ	Responders/actors
Last-mile local alerting, readiness, response, and public info	Municipal CP HQ / municipal services	Municipal leadership (not specified)	County CP HQ	Public

E) Bottlenecks / unclear points

- Public warning approval chain (who signs off public text; how updates/cancellation are authorised and versioned) is not specified.
- Update/stand-down governance is not explicitly mapped.

- Activation-by-level matrix (what exactly becomes mandatory at yellow vs orange vs red) is not detailed.

F) Data note

The fiche is supported by partner input specifying: legally responsible institutions (national technical bodies and CP/112 governance), county and municipal roles for operationalisation, the warning level schemes used (DHMZ colours; Croatian Waters flood phases), and the set of public warning channels (112 alerts, SMS/CBC in specific cases, media, municipal channels, sirens in selected municipalities).

6.10 Public Institution Development Agency of Lika-Senj County- LIRA (PP10- Croatia)

A) Role in the EWS chain

Type C – Support / county ecosystem stakeholder (not an alert issuer)

Lika-Senj County operates within Croatia's national multi-hazard EWS. Technical warnings originate from national competent bodies (DHMZ; Croatian Waters) and are operationalised through the Civil Protection Directorate / 112 system. At the territorial level, the Lika-Senj County Civil Protection Headquarters coordinates county readiness and distributes warnings to municipalities, supported by the Regional Civil Protection Service Gospić / Regional 112 Centre in Gospić as an operational contact point. LIRA participates indirectly by supporting data collection, risk assessment activities, stakeholder coordination and awareness initiatives, but is not an operational EWS authority.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: national monitoring/forecasting networks operated by DHMZ and Croatian Waters.
- Validation: technical verification performed by DHMZ and Croatian Waters using their IT platforms/models.
- Classification: warnings communicated through DHMZ colour-coded system (yellow/orange/red) and Croatian Waters flood alert phases (regular and emergency flood defence levels), alongside operational messages distributed via civil protection channels.

- Authorisation: operational routing/activation led through the Civil Protection Directorate / 112 system; county-level coordination is performed by the County Civil Protection Headquarters.
- Dissemination: national 112 system routes warnings and operational messages to the County Civil Protection HQ, municipalities and responders; public warning is described through a multi-channel set (112 public alerting, SMS/CBC in specific cases, media broadcasts, municipal websites/social media, telephone notifications to critical institutions, and sirens in selected municipalities).
- Activation/escalation: municipalities and local responders (including local fire brigades) implement local alerting, readiness and response actions under local plans; LIRA may support coordination/awareness tasks but does not command activation.

Data completeness note: approval/sign-off steps for public-facing message text (alert/update/cancel) and explicit update/stand-down decision rights are not specified in available sources.

C) Activation matrix (alert level × activated structures)

Level-by-level activation thresholds are not specified in available sources; the partner input confirms warning level taxonomies and the multi-level dissemination/implementation chain.

Warning reference in partner input	National 112 / CP Directorate	Regional 112 Centre (Gospić)	County CP HQ	Municipal CP HQ + responders
DHMZ (yellow/orange/red) + Croatian Waters flood phases	Yes	Yes	Yes	Yes (fire brigades as needed)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Issue meteo/hydro warnings & classify level	DHMZ / Croatian Waters	DHMZ / CW	CP Directorate / 112	Counties / municipalities
Route operational messages / trigger activation	CP Directorate / 112 system	CP Directorate	DHMZ / CW	County CP HQ, municipalities, responders

County readiness & coordination	County CP HQ	County CP HQ	Regional 112 Centre	Municipalities
Local protective measures & local public notice	Municipal CP HQ / local responders	Local municipal leadership (not specified)	County CP HQ	Public
Support (data collection / risk assessment / awareness)	LIRA	LIRA (within mandate)	County CP HQ / partners (as applicable)	Stakeholders

E) Bottlenecks / unclear points

- Public warning message approval chain (who approves/versions public text for alert/update/cancel) is not specified.
- Update/termination (stand-down) decision rights and procedures are not explicitly mapped.
- Channel-by-level mandatory rules (which channel is compulsory at which alert level) are not specified.

F) Data note

Supported by partner input describing: the national–county–municipal governance chain; county operational contact points (Regional 112 Centre Gospić / Regional Civil Protection Service Gospić); warning level schemes (DHMZ colours; Croatian Waters flood phases); and the set of public warning channels used locally. LIRA's role is explicitly recorded as indirect support (data/risk/awareness), without issuer or command authority.

6.11 Dubrovnik-Neretva Region (PP11- Croatia)

A) Role in the EWS chain

Type A – Coordinator/responder (county-level operationalisation of nationally issued warnings)

Dubrovnik-Neretva County is described as operating within Croatia's national multi-hazard EWS. Technical warnings originate from national competent bodies (DHMZ; Croatian Waters and other listed national monitoring bodies), while operational routing and instruction flows are linked to civil protection/112 structures. County and local civil protection headquarters implement preparedness and response actions at territorial level.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: national monitoring/forecasting networks operated by competent institutions (e.g., DHMZ and Croatian Waters; other hazard-monitoring bodies referenced).
- Validation: technical verification performed by competent national institutions using their own IT platforms.
- Classification: warning levels are described as a colour scale from green to red and linked to the national MeteoAlarm context; detailed local mapping of level-to-action is not specified in available sources.
- Authorisation: the operational trigger/routing is referenced through civil protection/112 structures; county decision rights vs 112 instruction rights are not detailed in available sources.
- Dissemination: partner input describes use of phone calls, social media and e-mails for public warning; SMS testing is reported; communication to the public is also described via official web pages and mobile apps (e.g., HRT METEO, NIS) and other media.
- Activation/escalation: county and local headquarters / responders implement measures under plans and national rules; level-by-level activation thresholds are not specified in available sources.

Data completeness note: a detailed step-by-step decision tree and level-by-level activation matrix are not provided; governance references rely on national rules and cited institutions rather than local procedural detail.

C) Activation matrix (alert level × activated structures)

Not specified in available sources (no level-by-level activation mapping provided).

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Issue meteo/hydro warnings / define warning level	Competent national bodies (e.g., DHMZ/CW)	Not specified in available sources	Civil protection/112 structures (referenced)	Counties/municipalities

Disseminate / route alerts and instructions	Not specified in available sources	Not specified in available sources	Not specified in available sources	Not specified in available sources
County/local operationalisation and measures	County/local HQ (referenced)	Not specified in available sources	112/civil protection structures (referenced)	Public / stakeholders

E) Bottlenecks / unclear points

- Alert level taxonomy is described generally (colour scale), but local level-by-level activation and mandatory thresholds are not specified.
- Public message authorisation/sign-off vs operational instruction routing is not differentiated in available sources.
- County decision rights vs 112 instruction rights are not described in sufficient detail for strict benchmarking.

F) Data note

Partner input provides evidence on (i) reliance on national competent institutions and their IT platforms, and (ii) multi-channel public warning practices (calls, e-mail, social media, SMS testing, official web/apps and media). However, governance detail on local decision gates and activation-by-level remains limited in available sources.

6.12 Karlovac County Fire Association (PP12 – Croatia)

A) Role in the EWS chain

Type B – Responder (firefighting operational response and coordination).

VZKZ operates as a responder within Croatia's multi-level civil protection system. Warnings are issued by national competent bodies (DHMZ; Croatian Waters) and routed through the civil protection / 112 chain to county/local structures. Fire services are activated as an operational arm once instructed, and then coordinate field response and reporting through established HQ interfaces.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: national monitoring/forecasting networks (DHMZ; Croatian Waters).
- Validation: performed by national competent bodies using their IT platforms/models.
- Classification: DHMZ colour-coded warnings (yellow/orange/red) and Croatian Waters flood alert phases (regular/emergency flood defence levels) are referenced as the warning schemes used; operational messages are distributed to county/local authorities via civil protection channels.
- Authorisation: operational routing/activation is issued through the Civil Protection Directorate / 112 system; VZKZ does not authorise alerts.
- Dissemination: warnings/instructions reach county and local structures through 112 and civil protection HQs; public warning channels are outside the responder's mandate (institutional/public channels are described at system level).
- Activation/escalation: fire brigades deploy and scale operations based on alerts/instructions and field conditions; coordination and situation reporting occur through HQ interfaces.

C) Activation matrix (alert level × activated structures)

Alert level / warning reference	Responder activation (VZKZ / fire brigades)
DHMZ colours; Croatian Waters flood phases	Conditional on alerts/instructions; scaling based on operational needs (level-by-level triggers not specified)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Dispatch firefighting resources	Fire brigade	Fire commander	County CP HQ / 112	Municipalities

Provide field updates / situation reports	Fire brigade	Fire commander	County CP HQ	112 / CP Directorate (as applicable)

E) Bottlenecks / unclear points

- No mapping of how warning levels translate into predefined fire service readiness modes.
- Interfaces for multi-agency incidents (who calls whom first; coordination sequencing) are not specified in available sources.
- Termination/demobilisation authority and stand-down criteria are not described.

F) Data note

Appropriate for responder mandate; contributes primarily to activation/escalation and operational decision points once the alert exists. The partner input confirms the national warning schemes used and the multi-channel public warning environment, but does not provide a responder-specific readiness-by-level protocol.

6.13 Ruđer Bošković Institute (PP13 – Croatia)

A) Role in the EWS chain

Type C – Support / scientific-technical contributor (no alert issuance authority)

RBI is positioned as a potential support node in the broader Croatian EWS ecosystem. The partner input primarily describes national institutions legally responsible for EWS activation, operation and communication (e.g., Civil Protection Directorate/112, DHMZ, Croatian Waters, HRT under protocol), while RBI itself is not described as an issuer or operational commander. RBI's role is therefore recorded as support-only: provision of scientific/technical inputs when requested, without assigning alert-issuing or dissemination authority.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: competent authorities' monitoring systems for multi-hazard events (e.g., meteo/hydro and other hazards referenced).
- Validation: performed by competent authorities (e.g., DHMZ / Croatian Waters, as described).

- Classification: national warning levels are described via DHMZ notices and MeteoAlarm colour coding (green/yellow/orange/red), with routing through national and territorial civil protection structures.
- Authorisation: operational communications about disasters are attributed to civil protection/112 structures; RBI has no authorisation role described.
- Dissemination: official channels include 112 structures and media transmission under protocol (HRT), plus other listed public channels; RBI has no dissemination authority described.
- Activation/escalation: responders and territorial HQs activate under civil protection governance; RBI may contribute technical knowledge/analysis if engaged, but triggers for engagement are not defined.

C) Activation matrix (alert level × activated structures)

Not applicable (support role; no activation-by-level mandate described for RBI).

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Provide scientific/technical analysis when requested	RBI	RBI	CP/112 (as requester)	Partners / relevant authorities

E) Bottlenecks / unclear points

- Trigger conditions and formal interface for requesting RBI support are not defined in available sources.
- Data-sharing protocols during emergencies (access rights, formats, timeliness) are not specified.
- RBI's formal position (on-call vs ad hoc consultative) is not described.

F) Data note

Partner input provides strong system-level context on Croatian EWS institutions, channels, and interoperability references, but does not describe RBI-specific operational procedures or formalised support activation protocols. The fiche therefore remains explicitly support-only.

6.14 Fire Department of the Istrian Region (PP14 – Croatia)

A) Role in the EWS chain

Type B – Responder (firefighting operational response and coordination)

VZIZ operates within Croatia's national multi-hazard EWS as a responder organisation responsible for operational firefighting response once warnings/instructions are issued through the civil protection chain. National technical warnings (DHMZ; Croatian Waters) are routed via the Civil Protection Directorate / 112 system to county and municipal structures; at county level, decision coordination is linked to the Istria County Civil Protection Headquarters and the Regional 112 Centre in Pazin. Partner input also references the County Fire Operations Center (ŽVOC Pula) as structured and equipped to function as the County Operational-Communication Centre of the County Civil Protection HQ (ŽOC CZ IŽ) for official communications and operational continuity.

B) Decision tree

detection → validation → classification → authorisation → dissemination → activation/escalation (incl. updates/stand-down)

Scheme (as described):

- Detection: national monitoring/forecasting networks (DHMZ; Croatian Waters) covering key hazards.
- Validation: technical verification performed by national competent bodies using their IT platforms/models.
- Classification: warning levels communicated through DHMZ colour-coded system (yellow/orange/red) and Croatian Waters flood alert phases (regular and emergency flood defence levels), plus operational messages distributed via civil protection channels.
- Authorisation: operational routing/activation led through the Civil Protection Directorate / 112 system; VZIZ does not authorise alerts.
- Dissemination: national 112 system routes warnings to the County CP HQ and Regional 112 Centre in Pazin, then to municipal HQs and emergency services; public warning is described through a multi-channel set (112 public alert system, SMS/CBC in specific cases, media broadcasts, municipal websites/social media, telephone notifications to critical institutions, and sirens in selected municipalities).
- Activation/escalation: fire brigades mobilise and coordinate response through VZIZ structures and ŽVOC/ŽOC interfaces as required; municipal/local structures handle last-mile public communication and immediate protective measures.

Data completeness note: level-by-level predefined triggers for responder readiness modes and stand-down authority are not specified in available sources.

C) Activation matrix (alert level × activated structures)

Alert level / warning reference	Responder activation (VZIZ / fire brigades)
DHMZ colours; Croatian Waters flood phases	Conditional on alerts/instructions; scaling based on operational needs (no level-by-level readiness protocol specified)

D) Mini-RACI (key decisions)

Decision	R	A	C	I
Dispatch firefighting resources	Fire brigade / VZIZ structures	Fire commander / VZIZ lead (as applicable)	County CP HQ / 112	Municipalities
Operational-communication continuity (ŽOC function)	ŽVOC Pula	County CP HQ	Regional 112 Centre (Pazin)	Relevant authorities/actors
Provide field updates / situation reports	Fire brigade	Fire commander	County CP HQ	112 / CP Directorate (as applicable)

E) Bottlenecks / unclear points

- No mapping of how warning levels translate into predefined fire service readiness modes.
- Interfaces for multi-agency incidents (coordination sequencing across services) are not specified in available sources.
- Termination/demobilisation authority and stand-down criteria are not described.

F) Data note

Supported by partner input describing: Istria's operation within the national EWS; the warning level schemes used (DHMZ colours; Croatian Waters flood phases); the set of public warning channels; and the governance feature of ŽVOC Pula functioning as a county operational-communication node (ŽOC CZ IŽ). The fiche is responder-focused and does not attribute alert-issuing authority.

7. Comparative synthesis and benchmarking

This chapter consolidates the Partner fiches into a comparative benchmarking view focused on governance and decision-making during an EWS alert. The objective is to highlight comparable governance features across territories, identify recurring decision-chain bottlenecks evidenced in available sources, and extract transferable “best practice seeds” that may support future harmonisation and interoperability within the Programme Area.

Benchmarking is conducted using the reference chain-of-command model (Chapter 4) and the fiche typology (Section 5.0). Comparative matrices rely primarily on Type A (Issuer/Coordinator) fiches. Type B (Responder) and Type C (Support) fiches are used to complement the analysis by documenting activation/escalation interfaces and support governance, without attributing alert-issuing authority where it is not mandated. Where a fiche did not specify an element, the entry is reported as “Not specified in available sources”.

7.1 Benchmarking matrix

Table 3 provides an extract of the governance benchmarking matrix using four comparability lenses:

- **Technical validation:** who verifies/validates the alert signal and assessment before classification/authorisation;
- **Approval/authorisation steps:** how many governance “gates” typically separate technical assessment from an officially authorised alert (including co-signature/managerial authorisation where described);
- **Public warning interface:** who is primarily responsible for public-facing communication and last-mile guidance;
- **Activation at higher severity:** which coordination structures and operational postures are systematically activated when severity increases (where the link to levels/phases is specified).

For clarity, “approval steps” are reported as a functional count based on available sources (e.g., technical assessment - co-signature/authorisation - issuance/dissemination), and are not intended as a legal audit of procedures

Table 3. Governance benchmarking matrix (extract)

Territory / system	Who verifies the alert (technical validation)	Typical approval steps (technical - authorised alert)	Primary public communicator (last-mile)	Structures activated at higher severity
Emilia-Romagna (PP2)	ARPAE–SIMC Functional Centre (CF) + SGSS validate (integrated evaluation).	Typically 2 (technical assessment + co-signature/co-issuance).	Municipal authority (Mayor/COC) for last-mile guidance; region publishes bulletin and institutional notifications.	COR strengthened (incl. H24 presidium where described); Prefecture/CCS for severe events; municipal COC as needed; specialised flood actors engaged.
Abruzzo (PP3)	Regional Functional Centre validates; alert issuance within the regional multi-risk alerting system.	Typically 1–2 (issuance within regional system + scale-driven activation/ordinance decision points).	Municipal authority (Mayor as local CP authority) for local protective actions; public-facing approval chain not specified.	Scale-based escalation: COC - CCS - COR - CON (depending on territorial scale).
Molise (PP4)	Regional Functional Centre validates (national functional-centre network).	Typically 2 (functional-centre output + regional CP/operative-room dissemination).	Not specified in available sources (public-warning governance not detailed).	SOR coordinates/manages emergencies; downstream activation (municipalities/Prefecture structures) described “as needed” (not mapped level-by-level).
Marche (PP5)	Regional Functional Centre validates (national functional-centre network); operative room supports dissemination.	Typically 2 (functional-centre output + operative-room dissemination / COR governance).	Municipal authority for local protective measures; public-	COR/crisis unit + H24 operative room; municipal activation per local plans; thresholds not specified level-by-level.

			message sign-off not specified.	
Veneto (PP6)	CFD validates (ARPAV provides monitoring inputs).	Typically 2 (functional-centre technical output + operative-chain dissemination/coordination).	Municipal authority/Mayor communicates local phase activation and guidance (channels vary by municipality).	SOR coordination + SSV 24/7 interface; COR/crisis unit as needed; municipalities activate/adjust local phases.
Puglia (PP7)	CFD validates national forecasts + regional monitoring and correlates thresholds/impacts.	Typically 3 (technical assessment - Director authorisation - official issuance/dissemination).	Municipal authority/Mayor for last-mile public warning; Region disseminates institutional alert via official channels.	SOIR coordination (24/7); CCS and COC activated for Yellow/Orange/Red (as described); wildfire coordination structures where applicable.
Zadar County (PP8 – Croatia)	Technical verification/classification by national competent bodies (DHMZ; Croatian Waters).	Typically 2 (national technical warning - CP Directorate/112 routing/coordination). County operationalisation follows.	Local/municipal channels + 112 public alerting; public text sign-off not specified.	112 system + Regional 112 Centre (Zadar) as operational hub; County CP HQ; municipal HQ and responders; ŽVOC supports official communications/continuity (as described).
Split-Dalmatia County (PP9 – Croatia)	Technical verification/classification by DHMZ; Croatian Waters (plus other national hazard bodies listed in input).	Typically 2 (national technical warning - CP Directorate/112 routing/coordination).	Local/municipal channels + 112 public alerts; public text sign-off not specified.	County CP HQ + municipal structures; responders activated through procedures; firefighting activation/coordination via ŽVOC (as described).

Lika-Senj County (PP10 – Croatia; partner is a support actor)	Technical verification/classification by national competent bodies (DHMZ; Croatian Waters).	Typically 2 (national technical warning - CP Directorate/112 routing/coordination). County/local operationalisation follows.	Not specified in available sources (county-to-municipality "last mile" channel mix not detailed).	112 routing + county/local CP HQ readiness; responders (incl. fire brigades) activated as needed; level-by-level triggers not specified.
Dubrovnik-Neretva County (PP11 – Croatia)	Technical verification/classification described via national colour-scale warning system (DHMZ) and national competent bodies.	Not specified in available sources as a step-by-step county workflow (national rulebooks referenced).	Public communication channels described at system level (official web pages, mobile apps, SMS, radio/TV); county-level sign-off not specified.	Not specified in available sources (activation matrix by level not provided).

Note: Croatian county fiches reflect county-level operationalisation of nationally issued technical warnings (DHMZ; Croatian Waters) routed through the Civil Protection Directorate/112 system. Where partner inputs do not specify level-by-level thresholds, matrices record structures functionally and mark missing elements as "Not specified in available sources".

7.2 Comparative findings by governance dimension

Who verifies the alert?

Across partner territories, technical verification is typically assigned to functional/technical bodies that consolidate monitoring data, forecasts, and threshold/impact assessments. The institutional form of verification and the handover to authorisation varies:

- In several Italian regional fiches, verification is performed by Regional Functional Centres (or equivalent technical services), with issuance either integrated into the same structure or formalised through a co-signature/dual-signature mechanism (where documented).
- In other cases, technical verification is followed by a distinct authorisation gate (managerial/civil protection authorisation) before an alert becomes official (clearly documented in Puglia).
- In Croatian county fiches, technical verification/classification is described as performed by national competent bodies (DHMZ; Croatian Waters), while the operationalisation and routing of warnings occurs through the Civil Protection Directorate/112 system and county/local civil protection structures.

How many approval/authorisation steps?

The number of authorisation steps affects both robustness and speed. Two-step patterns are frequently described where technical outputs are disseminated through an operative room/centre and regional civil protection governance, while some territories report an additional explicit authorisation step prior to issuance:

- Two-step patterns can support rapid dissemination but require clear accountability markers, particularly for update/downgrade/termination decisions (often not specified in available sources).
- Three-step patterns (e.g., Puglia: technical assessment - Director authorisation - issuance) can strengthen traceability and decision ownership but can introduce delay unless delegation/backup arrangements are clearly defined (not specified in available sources).

- Scale-based escalation models (e.g., Abruzzo) add decision points during escalation even where base alert issuance is relatively streamlined.

Who communicates to the public?

Partner fiches indicate that public communication frequently relies on a last-mile municipal function, even where regional systems publish official bulletins and notify institutions. This governance feature is critical for benchmarking because it affects message consistency and actionability:

- Several Italian regional fiches explicitly associate municipalities (often Mayor/COC) with local protective actions and last-mile public guidance, while regional bodies focus on bulletin publication and institutional dissemination.
- In Croatian fiches, public-facing communication is described as combining national/system channels (e.g., DHMZ public warnings; 112/public alerting) with locally implemented municipal channels; however, approval/versioning of public-facing message text (alert/update/cancel/stand-down) is not specified.

Which structures are activated at higher severity?

Across territories, increased severity typically triggers more formal coordination structures and strengthened operational postures (e.g., H24 operative rooms, crisis units, prefecture/provincial coordination mechanisms). However, the link between alert levels and mandatory activation thresholds is not always specified level-by-level:

- Regional operational rooms (SOR/SOIR-type) and coordination/crisis bodies (COR) appear as recurring backbone structures in multiple Italian partner territories.
- Prefecture-led coordination (e.g., CCS) is emphasised for severe events in several Italian fiches (explicit in Emilia-Romagna; structurally central in scale-based models).
- In Croatian county fiches, 112 operational functions and county/local civil protection headquarters are described as backbone escalation nodes, with responders (including firefighting units, in counties where described) activated through established procedures; level-by-level mandatory thresholds are often not specified.

7.3 “Best practice seeds” for harmonisation

Based on the mapped governance patterns, the following elements emerge as transferable “best practice seeds” that may support harmonisation across the Programme Area. These are candidates for common guidance/templates/minimum governance standards and are not presented as mandatory requirements:

1. Explicit separation of technical verification and formal authorisation (where applicable). Distinguishing technical assessment from formal authorisation strengthens accountability and clarifies decision rights.

2. Joint verification/issuance arrangements with clear traceability. Co-signature/co-issuance mechanisms can reduce ambiguity on alert ownership and support auditable decision chains.

3. Defined 24/7 operational posture linked to higher alert levels/phases. Where documented, explicitly linking H24 presidium/operative-room strengthening to severity supports readiness and predictable escalation.

4. Structured escalation architecture linked to scale and severity. Clear escalation ladders (municipal–provincial–regional–national; or county–municipal with national routing) help benchmark "what changes when severity increases" and improve interoperability.

5. Clear last-mile public warning responsibility supported by message lifecycle logic. Explicit last-mile roles (often municipal) combined with standard governance for Alert / Update / Downgrade / Cancel / Stand-down messaging improves public communication consistency across territories and channels.

7.4 Preliminary gaps impacting governance comparability

The benchmarking exercise identifies constraints affecting strict comparability across territories as reflected in available sources. These are reported descriptively and transparently, without inferring missing elements:

- Public communication responsibilities are not always explicitly defined (e.g., differentiation between public message approval and last-mile guidance ownership).
- Approval/authorisation steps are sometimes implied rather than stated, limiting consistent benchmarking of speed versus control.
- Activation thresholds for higher-level structures (e.g., when COR, CCS, COC becomes mandatory; or when county-level posture shifts under national warnings) are often described qualitatively rather than mapped to alert levels/phases.
- Delegation/backup rules (substitution for key decision-makers), decision logging, and versioning practices for updates/termination are inconsistently described across partner inputs.

8. Gaps and missing elements (governance-focused)

This chapter summarises governance-related gaps and elements not specified in available sources identified through the partner/regional fiches (Chapter 6) and the comparative benchmarking synthesis (Chapter 7). The intent is to highlight issues that may reduce the clarity, efficiency, and reliability of the chain of command during time-critical EWS alert situations.

In line with the scope of this document, the gaps below focus strictly on decision-making and governance arrangements (decision rights, authorisation, escalation, accountability, documentation and traceability). Technical platform and instrument issues are deliberately excluded and are addressed in the complementary deliverable *Mapping report on existing EWS*.

8.1Gaps in decision rights and sign-off clarity

A recurring governance constraint across territories is that "who has the final decision" is not always explicitly articulated at each critical decision gate. While several partners clearly describe institutional dissemination chains (e.g., functional centre - operative room/coordination body - municipalities), the formal sign-off point is not consistently specified for the following decisions:

- Issuance and level changes (upgrade/downgrade): in multiple fiches, alert changes are described operationally but not always as a formal authorisation step with a clearly identified accountable authority (particularly for update cycles over time).
- Public warning content approval: responsibilities for approving final public-facing messaging (text, protective instructions, timing) are sometimes implicit, especially where last-mile communication is decentralised to municipal actors.
- Termination / stand-down ("all clear"): who decides that an alert is terminated or stood down, and how that decision is communicated and recorded, is frequently under-described in available sources.

Governance element frequently not specified in available sources: a concise statement of decision rights indicating who is Accountable for issuing the alert, changing the level, approving public warning content, and terminating/standing down the alert (including update/cancellation messages).

8.2 Limited documentation of delegation and replacement rules

Even where governance structures are clearly described (e.g., operative rooms, crisis units, prefectural coordination bodies, 112 operational hubs), partner inputs frequently do not specify delegation, substitution, or replacement arrangements. This represents a governance

vulnerability in real-world emergencies, where key roles may be unavailable due to parallel incidents, staffing limits, or continuity constraints.

Elements frequently not specified in available sources include:

- Who formally substitutes a decision-maker when the primary accountable role is unavailable (including out-of-hours or multi-day events);
- Whether predefined backup contacts/roles exist for authorisation and public communication;
- Whether authorisation rights for alerts/messages can be delegated, and under which conditions.

Governance element frequently not specified in available sources: a basic deputy/backup rule for each key decision gate, including the conditions under which substitution applies.

8.3 Fragmentation in “last-mile” public warning responsibilities

The fiches indicate that last-mile public warning is often managed at the municipal level, which is consistent with subsidiarity and local preparedness planning. However, decentralisation can create governance gaps when roles and interfaces are not formally described, including:

- Unclear authorisation boundaries for public communication (e.g., whether the Mayor is the sole authorised public voice, or whether other bodies can issue public statements and under what conditions);
- Heterogeneous tools and channels across municipalities without a minimum common logic for message consistency, timing, and linkage to the official alert bulletin;
- Unclear rules for alignment between local guidance and regional/national alert content, particularly during multi-municipality events and rapidly evolving situations.

These gaps can lead to uneven public reach and potential inconsistencies in protective instructions across neighbouring municipalities during the same event.

Governance element frequently not specified in available sources: an explicit description of how last-mile public warning is coordinated during multi-municipality events (including minimum message-content linkage to the official alert bulletin and the role responsible for alignment).

8.4 Escalation and activation triggers not consistently formalised

Across multiple territories, escalation and activation structures are clearly named (e.g., COR/SOR/SOIR, Prefecture/CCS, municipal COC; in Croatia: Civil Protection Directorate/112 nodes, county/local headquarters, ŽVOC/operational-communication functions). However,

the governance logic linking severity/levels to mandatory posture changes is not always documented in a level-by-level format.

Elements frequently not specified in available sources include:

- Clear activation thresholds that make coordination structures mandatory (e.g., when COR/CCS/COC becomes compulsory rather than “as needed”);
- Explicit rules for vertical escalation (local - provincial/prefecture - regional - national, or county - national routing) and who triggers it under which conditions;
- Clear mapping of posture changes (e.g., H24 presidium, duty officer reinforcement, continuity arrangements) to alert levels/phases;
- Explicit governance for escalation during updates, i.e., who decides and communicates changes as forecast confidence and impacts evolve.

Governance element frequently not specified in available sources: a level/phase-linked activation and escalation rule-set that indicates when each coordination body must be activated and how escalation decisions are authorised and communicated.

8.5 Incomplete decision logging, versioning, and audit trail practices

For interoperability and accountability, it is important that alert decisions and message changes (Alert/Update/Downgrade/Cancel/Stand-down) are traceable and consistently versioned. Across fiches, formal references to SOPs and procedures exist in several cases, but detailed decision logging/audit trail practices are not consistently documented.

Elements frequently not specified in available sources include:

- Whether a decision log is maintained (who records what, in which format, and where it is stored);
- How message versioning is managed across institutional notifications and public-facing messages to avoid contradictory communication;
- Whether stand-down decisions trigger a formal closure practice (e.g., situation report closure, closure entry, after-action review trigger).

Governance element frequently not specified in available sources: a minimum decision-log and message-versioning practice that captures time, decision-maker, basis, recipients/channels, and version identifiers for Alert/Update/Cancel/Stand-down.

8.6 Variability in completeness of governance information across partners

A practical constraint affecting benchmarking is that some fiches provide rich governance detail (roles, structures, channels, decision gates), while others provide only high-level

references to national rules/frameworks without specifying operational decision points. This variability reduces cross-territory comparability and limits the degree to which certain benchmarking dimensions can be interpreted consistently across all partner territories.

Governance element frequently not specified in available sources: a consistently specified minimum governance dataset for mapping (decision gates, accountable actors, activation structures, escalation triggers, public warning interface, and update/stand-down governance), as defined in Chapter 4.

Summary of priority governance gaps (cross-territory)

Across the Programme Area, the governance gaps that most directly affect the chain of command during EWS alerts, as evidenced by available sources, are:

- Implicit or unclear sign-off for issuing, upgrading/downgrading, terminating/standing down alerts, and approving public warning content;
- Missing delegation/substitution rules for key decision-makers and authorising roles;
- Fragmented last-mile public warning interfaces where responsibilities and alignment rules are not explicitly described;
- Escalation and activation triggers not consistently linked to alert levels/phases and posture changes;
- Limited description of decision logging and message versioning, affecting traceability and coherence across Alert/Update/Cancel/Stand-down communications.

These points provide a governance-focused baseline for subsequent REALIST work on harmonisation and cross-border operability, while technical upgrades and platform interoperability considerations remain within the scope of the complementary *Mapping report on existing EWS* and later technical activities.

9. Conclusion

This deliverable mapped the governance and decision-making structures activated during an EWS alert across the REALIST partner territories in the Interreg Italy–Croatia Programme Area. Using a common reference chain-of-command model, the analysis documented "who decides what, when, and under which activation arrangements" across the alert lifecycle, including decision gates for issuance, updates, escalation/downgrade, and stand-down, as well as the interface to public warning and last-mile communication. Partner inputs submitted after the initial consolidation cycle were integrated using the same fiche template and validation rules to preserve comparability and traceability.

The mapping confirms that, despite differences in institutional terminology and administrative organisation, partner territories can be described through a shared set of functional governance steps: technical detection and validation, classification, authorisation, dissemination, and activation/escalation. In the Italian partner territories, governance is frequently characterised by structured regional arrangements involving functional/technical centres, regional civil protection coordination structures (operative rooms and coordination/crisis bodies where described), and municipalities as key last-mile implementers, often with the Mayor as the public-facing authority for local protective actions. In the Croatian partner inputs, governance is characterised by nationally anchored technical warning sources operationalised through the civil protection chain, with the Civil Protection Directorate/112 interfaces acting as a central routing and coordination touchpoint and county/municipal civil protection headquarters enabling territorial activation and responder mobilisation.

The comparative synthesis indicates that governance differences across territories are driven primarily by: (i) how decision rights are distributed between technical bodies and competent authorities; (ii) how many authorisation "gates" functionally separate technical assessment from official issuance (including co-signature or managerial authorisation where described); (iii) how public warning responsibilities are allocated between regional/national structures and municipal last-mile actors; and (iv) which coordination structures and operational postures are activated as severity increases (e.g., operative rooms, coordination/crisis bodies, prefecture-led coordination structures where described, and 112/county operational hubs in the Croatian context). Where explicitly documented, governance features such as clear co-signature/co-issuance arrangements, defined regional coordination hubs, and scale-based escalation ladders provide practical reference points for transferable governance strengthening approaches.

At the same time, the mapping identifies governance constraints affecting comparability and operational clarity, i.e., elements not consistently specified in available sources. These include: explicit sign-off for upgrades/downgrades and stand-down; delegation/substitution rules for key decision-makers; formalised activation and escalation triggers linked to alert levels/phases and posture changes; clearer differentiation between public message approval and last-mile guidance ownership; and decision logging/versioning practices across Alert/Update/Cancel/

Stand-down messages. These gaps do not pre-judge system performance; rather, they indicate where governance articulation and traceability can be strengthened to support consistent command-chain functioning under time pressure and reduce friction points relevant for cross-border coordination.

Overall, this deliverable establishes a structured governance baseline for REALIST *WP1. Benchmarking and assessment of existing Early Warning System (EWS)* by making decision pathways and command-chain interfaces comparable across partner territories. It provides an evidence-based foundation for subsequent work on identifying weaknesses and missing elements and for formulating actionable, Programme Area-relevant recommendations to support harmonisation and improved cross-border operability of EWS governance and alert management practices.