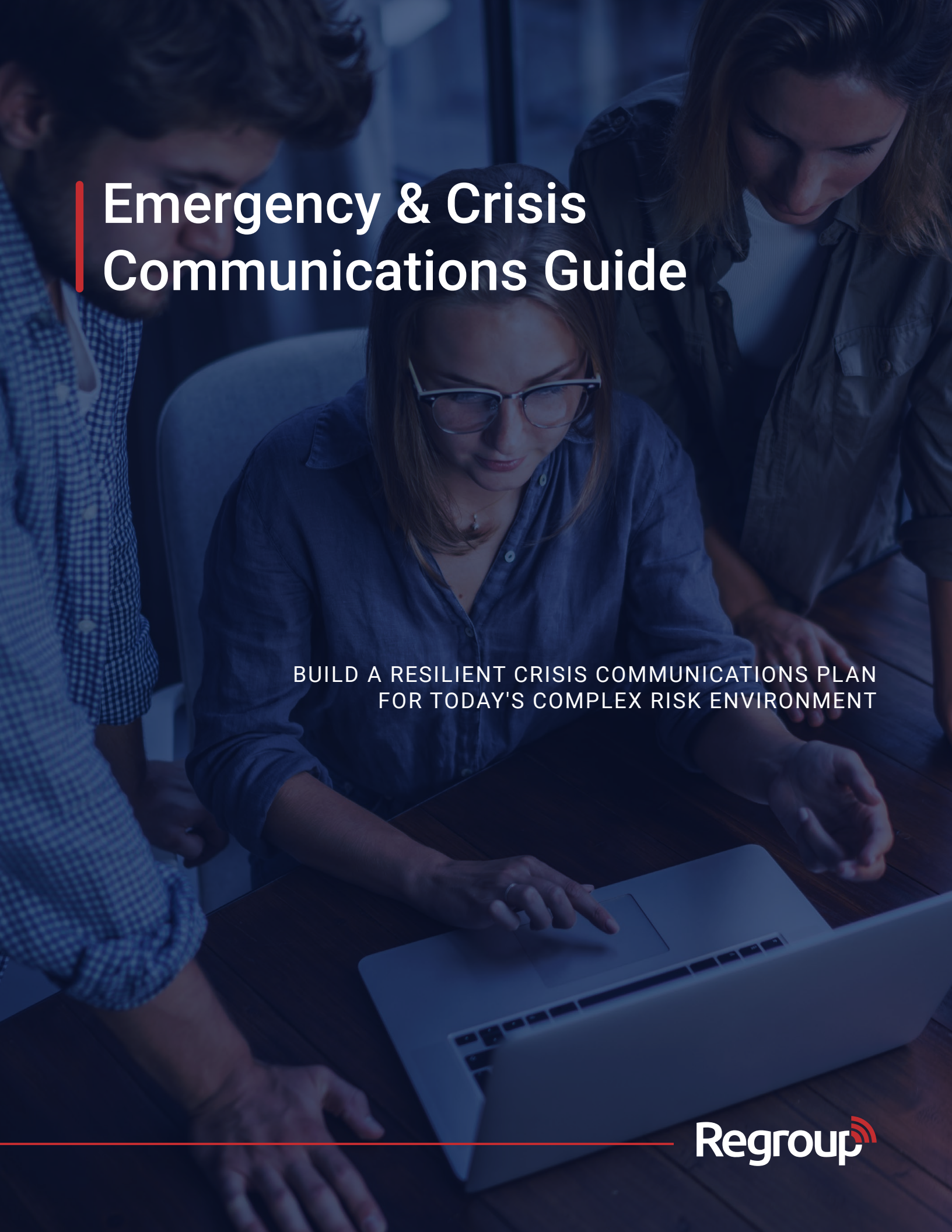


Emergency & Crisis Communications Guide

BUILD A RESILIENT CRISIS COMMUNICATIONS PLAN
FOR TODAY'S COMPLEX RISK ENVIRONMENT

Regroup

Table of Contents

Introduction **3**

The Modern Threat and Trend Landscape **4**

What Makes a Plan 6

Define Communication Activation Levels 6

Establish Governance, Roles and Decision Authority 7

Plan Execution **9**

Define Audience and Channel Strategy 9

Communicate Throughout the Incident 9

Recovery and Trust Repair 10

Evaluate Performance and Continuously Improve 10

AI in Crisis Communication **12**

Turn Emergency Communications Plans Into Action **13**

Bibliography **14**

Introduction

Crisis communication looks different than it did even two or three years ago. The triggers have multiplied — cyber incidents and technology failures now sit alongside severe weather and physical threats as leading causes of activation.

The response window has compressed from hours to minutes. Even the information environment itself has become contested: AI-generated deepfakes, bot-amplified narratives, and AI search summaries can all shape what people believe about an incident before your official statement is even drafted.

At the same time, the fundamentals haven't changed. Organizations that communicate well in a crisis are the ones that planned before the crisis, defining who has authority to act, which channels reach which audiences, what gets said in the first ten minutes, and how the organization repairs trust afterward.

Modern crisis communication is no longer simply about sending alerts. It is about delivering timely, accurate, clear, and audience-appropriate information through right channels while maintaining trust and situational awareness throughout an event.

This guide provides practical strategies, example frameworks, and planning considerations to help organizations strengthen their emergency and crisis communication programs, address emerging information challenges, and improve operational resilience.

The Modern Threat and Trend Landscape

The principles of crisis communication remain largely unchanged, but the environment in which crises unfold continues to evolve. The following trends are influencing how organizations approach emergency and crisis communication planning.

AI-Generated Disinformation at Machine Speed

Generative AI has made it easier to create convincing synthetic text, images, audio, and video. During an incident, misleading or fabricated content can complicate efforts to establish a shared understanding of what has occurred. Recent disasters have already shown this in practice: after Hurricane Helene, AI-generated fake images of storm damage circulated as a counterproductive tactic against response efforts and public relations, and during the early-2025 California wildfires, a fabricated deepfake image of the Hollywood sign engulfed in flames spread widely on social media, accumulating over a million views within 24 hours despite the image containing obvious errors.

Communication teams should establish procedures for verifying consequential information through trusted sources before incorporating it into official communications and for responding to significant misinformation when appropriate.

Compressed Response Windows

Response windows keep shrinking. Plans built around a 24-hour response cycle are increasingly out of step with how fast narratives now move, particularly as fragmented media and AI-driven information accelerate how quickly a story takes hold before an organization can respond.

Fragmented Media and Declining Institutional Trust

No single channel reaches an entire audience anymore. Owned channels, social platforms, and traditional media each reach different, overlapping segments — and trust in any single source, including "official" sources, is lower than it used to be.

A 2026 FGS Global survey found that 61% of people believe mainstream news media have their own agenda and cannot be trusted to report fairly, with only 53% trusting television news and 52% trusting newspapers as information sources. Only 41% of people trust big businesses, 38% trust big tech companies, and 37% trust government agencies. This makes redundant, multi-channel delivery a baseline requirement rather than a nice-to-have.

New Early-Warning Surfaces

Community platforms such as Reddit, Discord, and TikTok comment sections increasingly surface signals of a brewing crisis before it is reported anywhere official. Monitoring strategies built solely around news alerts and official social accounts now miss early signals that show up elsewhere first.

AI Search-and-Answer Engines are Part of the Narrative

What AI tools and AI-generated search summaries say about your organization during an active incident is now part of the information environment you have to manage — not just what journalists or social accounts say.

A July 2025 Associated Press-NORC poll found that 60% of Americans overall, and 74% of those under 30, use AI to find information at least some of the time — underscoring why monitoring how your organization is described in AI-generated answers is an emerging practice worth building into your communications workflow.

Cyber Incidents and Technology Failures as a Rising Trigger

Alongside weather and physical safety events, cyberattacks and technology outages increasingly require the same coordinated, rapid response that physical emergencies do.

FEMA's guidance on planning for cyber incidents notes that a cyber incident threatening or resulting in physical consequences may lead to a Stafford Act declaration and can call for a combined Cyber/Physical Unified Coordination Group, given the complex nature of cyber incidents and their potential for cascading impacts. This requires crisis communication plans to treat technical incidents with the same rigor as physical emergencies.

Employee Advocacy, Carefully Balanced

Employees can be credible, trusted voices during a crisis, but mobilizing them requires guardrails so they aren't overexposed, put at professional risk, or burned out by repeated crisis demands.

As Chambers and Partners' 2026 crisis management guide observes, speed and empathy matter as much as accuracy in a crisis response. A factual response delivered with the wrong tone can do as much damage as a delayed one.

What Makes a Plan

An Emergency and Critical Communications Plan transforms communication policies into actionable procedures. It defines how an organization communicates before, during, and after an incident by linking severity levels, decision authority, responsibility matrices, audience groups, communication channels, and message templates into a single operational framework.

An effective communications plan should answer six essential questions:

- When is the communications plan activated?
- Who has authority to approve and release communications?
- Who needs to receive information?
- Which communication channels should be used?
- What information should be communicated?
- How often should updates be provided throughout the incident?

Define Communication Activation Levels

Establishing communication activation levels in advance can help organizations scale their communication response as conditions change. A developing situation may initially require monitoring and internal coordination, while a major incident may require organization-wide notifications, executive involvement, public communications, and sustained updates.

The following model is a Regroup example framework designed to illustrate how communication activities might expand or contract according to an incident's scope and communication needs. The communication activation level should support — not replace — the organization's established process for classifying and managing the underlying incident.

Communication Level	Definition	Example
Organization-wide Activation **Level 1**	A major event requiring extensive communication across the organization and likely with external stakeholders.	Major disaster affecting multiple locations; significant organization-wide disruption
Localized Activation **Level 2**	A confirmed event requiring communication with a specific facility, location, department, or population.	Building evacuation; localized technology outage; facility disruption
Monitoring **Level 3**	A developing situation requiring monitoring and communication readiness but potentially limited initial notification.	Severe weather watch or advisory; developing operational issue
Operational Communication **Level 4**	An event that can generally be handled through established operational communication procedures.	Localized service disruption; temporary facility issue

This example is intended to help organizations develop their own framework rather than replicate a specific industry standard. Severity levels and escalation criteria should be tailored to your organization's risks, structure, and response processes.

Establish Governance, Roles and Decision Authority

Organizations should define in advance which authorized personnel can issue notifications without unnecessary approval delays, consistent with established policies and procedures.

Every role in a crisis communication plan should have a designated primary individual and at least one trained backup. **Uncertainty about who can approve communications is one of the most common causes of delay during an incident.**

The roles below are examples of functions that may participate in emergency and crisis communications. Organizations may use different titles, combine responsibilities, or assign additional roles based on their structure, industry, and established incident management procedures.

An example of communication authorities and approvals might look like this:

- **Incident Commander / Incident Lead**
  Coordinates the operational response according to the organization's incident management structure and provides or confirms operational information needed for communications.
- **Communications Lead**
  Coordinates communication planning and execution, develops messaging, determines communication channels, audiences and coordinates stakeholder communications.
- **Spokesperson / Public Information Function**
  Serves as the organization's public voice and delivers approved statements to the media and other external audiences.
- **Legal Counsel / Compliance Advisor**
  Advises on legal, regulatory, contractual, and privacy considerations when appropriate under the organization's established procedures.
- **Technical Subject Matter Expert (SME)**
  Provides technical expertise, verifies operational facts, and confirms the accuracy of information before release. Depending on the incident, this may be an IT manager, engineer, public health official, facilities director, or another technical expert.
- **Executive Leadership**
  Provides strategic oversight, approves communications for high-impact incidents, allocates organizational resources, and represents the organization during major crises.

This framework is provided as an example, not a prescriptive organizational model. Roles and tasks should be adapted to your organization's actual structure and validated with legal/compliance before adoption.

Incident Communication Roles and Responsibilities Matrix

A responsibility matrix can help organizations document who leads, supports, approves, or is notified for important communication activities during an incident. Clarifying these responsibilities in advance can improve coordination and reduce uncertainty when communication decisions must be made quickly.

Establishing distinct matrices for various emergencies enables organizations to create tailored communication frameworks that align with specific event types, required activation level, overall structure, and defined operational guidelines.

Example | **Communication Level 3 Activation: Monitoring**

Imagine an organization is monitoring a developing situation. The Communications Lead may coordinate communication readiness while the incident or operational lead monitors conditions and relevant subject-matter experts help validate incoming information.

Task	Incident Commander	Communications Lead	Legal Counsel	IT/Security Liaison/SME	Executive Leadership
Assess communication activation needs	Lead	Support	—	Support	Notify
Activate communication procedures	Support	Lead	—	—	Notify
Verify information before release	Support	Lead	—	Support	—
Draft initial alert or communication	Support	Lead	—	—	—
Identify audiences and channels	Support	Lead	—	Support	—
Send alert	—	Lead	—	—	Notify
Monitor for escalation triggers	Lead	Support	—	Support	Notify
Document decisions and actions	Support	Lead	Support	—	—

This serves as an initial template and a sample matrix from Regroup. Responsibilities should be adapted to your organization's actual structure and reviewed with leadership stakeholders and legal/compliance before adoption.

Plan Execution

Define Audience and Channel Strategy

An effective crisis communication plan recognizes that different audiences require different information, communication channels, and levels of detail. While the core facts should remain consistent, messages should be tailored to the needs and expectations of each audience.

Audience	Primary Channels	Message Focus	Special Considerations
Employees / staff	Mass notification app, SMS/Text, email, intranet, voice, desktop	What to do, safety status, where to get updates	Assume messages may be shared externally
Leadership / board	Established internal channels	Situational awareness, decisions requiring leadership involvement	Follow established escalation procedures
Public / community	Mass notification app, social media, SMS/Text, voice	Approved safety information, verified status, updates	Provide clear sources for continued updates
Media	Official statements, media channels	Verified facts, consistent spokesperson message	Communications may be quoted or redistributed
Families and affected individuals	Direct contact, dedicated hotline	Individual status, support resources, next steps	Consider privacy and highest sensitivity; avoid mass-channel-only contact

Channel selection should reflect the organization's audience, accessibility requirements, available technology, urgency, incident conditions, and established procedures.

Communicate Throughout the Incident

Crisis communication is a continuing process rather than a single notification. Depending on the incident and the organization's procedures, communication activities may include:

- **Initial Alert:** Notify affected audiences as quickly as possible with confirmed information and immediate protective actions.
- **Situation Updates:** Provide regular updates as conditions evolve, even if there is little new information to report.
- **Accountability Requests:** Use two-way communications to confirm recipient safety, gather situational information, and identify those requiring assistance.
- **Operational Instructions:** Share changes to facility status, work schedules, transportation, or service availability.
- **Recovery Communications:** Inform stakeholders when operations are being restored and communicate expectations during the recovery phase.
- **All-Clear Notification:** Clearly communicate when the immediate threat has ended and outline any remaining precautions or next steps.

Transparent communication helps reduce uncertainty, improve compliance with protective actions, and maintain stakeholder confidence throughout the event.

Recovery and Trust Repair

Communication responsibilities frequently continue after the immediate threat has passed. Organizations may need to explain what happened, communicate recovery progress, address stakeholder concerns, correct significant misinformation, and provide information about organizational improvements.

Depending on the circumstances, organizations should consider:

- Following through on commitments communicated during the incident.
- Providing updates until affected audiences have sufficient information about recovery or resolution.
- Acknowledging verified impacts and organizational actions clearly and appropriately.
- Coordinating required disclosures and reporting with qualified legal, compliance, regulatory, and operational personnel.
- Correcting significant misinformation when doing so will improve stakeholder understanding rather than unintentionally amplifying unsupported claims.

Evaluate Performance and Continuously Improve

Continuous improvement helps organizations build a more resilient communications capability and better prepare for future critical events. The emergency communications plan should be tested regularly to ensure people, processes, and technology perform as expected.

Exercises should evaluate communication speed, message clarity, approval workflows, technology performance, and cross-functional coordination.

Metrics to Consider

Metric	Why It Matters
Time to first message	Identifies delays between activation and communication
Delivery rate	Helps determine whether messages successfully reached intended endpoints
Response rate	Provides insight into recipient engagement where acknowledgement is requested
Audience coverage	Identifies potential gaps in recipient data or channel strategy
Approval/authorization turnaround	Identifies potential bottlenecks in communication workflows
Correction time	Measures how quickly inaccurate organizational communications or significant misinformation are addressed
Exercise participation and performance	Helps determine whether personnel understand and can execute the plan

Conduct an After-Action Review (AAR)

Every incident and exercise provides an opportunity to strengthen future communications. Following exercises and significant activations, evaluate:

- How quickly communications were initiated
- Whether messages reached intended audiences
- Delivery and acknowledgement rates
- Communication accuracy and consistency
- Effectiveness of communication channels
- Approval process efficiency
- Stakeholder feedback
- Lessons learned and improvement opportunities

Use these findings to update plans, templates, training programs, and communication strategies.

AI in Crisis Communication

Artificial intelligence is becoming part of the emergency management landscape, offering crisis teams new ways to process information, prepare communications, and respond more quickly as situations evolve.

AI can support teams by drafting messages for human review, translating approved communications, summarizing incoming reports and social activity, analyzing information from trusted forecasting sources, and helping identify emerging misinformation or stakeholder concerns.

AI should support—not replace—human judgment and organizational decision-making. Organizations should establish clear responsibility for reviewing and approving AI-assisted communications, verify critical information against authoritative sources, and protect sensitive data through appropriate cybersecurity and privacy controls.

Verifying Information Before You Alert

Misinformation tends to surface fastest on social media, exactly where emergency teams are also trying to detect real incidents. Use this sequence before any AI-surfaced or unconfirmed report shapes a notification.

Step 1: Source the Claim

- Is this from an official, verified account or channel (government agency, official news outlet, your own operations center)?
- If it originated on social media or from an AI summary, can you find independent corroboration?

Step 2: Check the Media

- For images/video: look for inconsistencies (odd lighting, warped text, unnatural movement) associated with AI generation.
- Run a reverse image search if the visual is central to the claim.

Step 3: Cross-Check with Internal Sources

- Compare against your own sensors, staff reports, or command center data before treating external claims as fact.

Step 4: Decide and Document

- If confirmed: proceed according to the organization's established communication and authorization procedures.
- If unconfirmed: continue verifying, and avoid amplifying the claim — including by publicly denying unverified rumors, which can spread them further.
- If false and circulating: consider whether an authorized correction or clarification is appropriate.

Turn Emergency Communications Plans Into Action

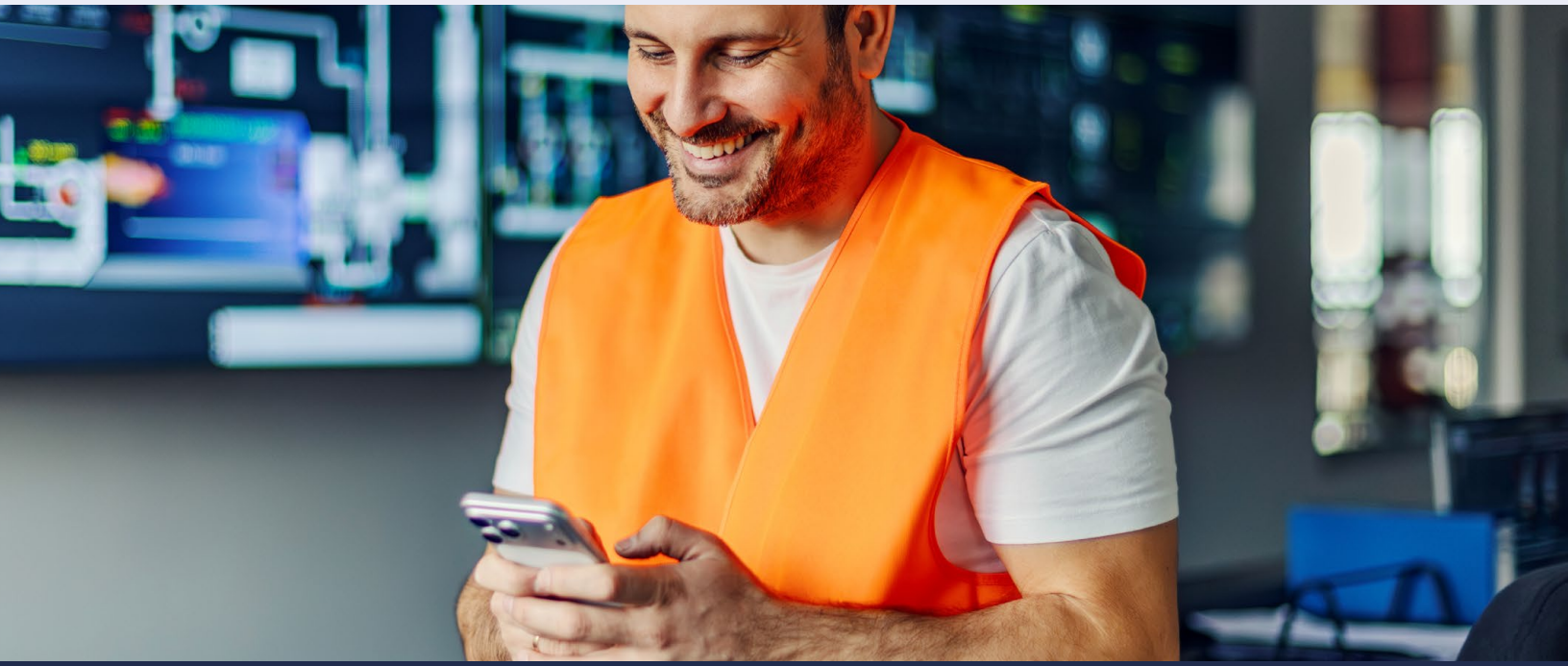
Effective crisis communication starts well before an incident occurs. Organizations that establish clear procedures, define responsibilities, train personnel, exercise their plans, and evaluate performance are better positioned to communicate effectively when an incident occurs.

Technology can help put those plans into action. Regroup's mass notification system supports established emergency communication procedures and reliable day-to-day communication with capabilities such as:

- Fast multi-channel emergency notifications
- Free mobile app
- Unlimited templates and groups
- Location-based messaging
- Automated NOAA weather alerts
- Automatic message translation across 130+ languages
- Two-way communications
- Polling and employee accountability
- Real-time analytics and incident reporting
- Open API integrations
- Role-based permissions

Regroup Incident Management's workspace extends this capability by providing a centralized environment for coordinating communication and response activities throughout an incident, from initial activation through resolution and recovery.

Together, these capabilities help organizations translate communication plans into repeatable workflows that can be activated, coordinated, and adapted as an incident evolves.



Bibliography

Bari, L.F., Ahmed, I., Ahamed, R., Zihan, T.A., Sharmin, S., Pranto, A.H., and Islam, M.R. "Potential Use of Artificial Intelligence (AI) in Disaster Risk and Emergency Health Management: A Critical Appraisal on Environmental Health." Environmental Health Insights, vol. 17, December 18, 2023. https://pmc.ncbi.nlm.nih.gov/articles/PMC10712270/

Centers for Disease Control and Prevention (CDC). "Crisis & Emergency Risk Communication (CERC) Manual." U.S. Department of Health and Human Services. https://www.cdc.gov/cerc/php/cerc-manual/index.html

Chambers and Partners (FGS Global). "Crisis Management 2026 – USA: Trends and Developments." Chambers and Partners Global Practice Guides, last updated March 24, 2026. https://practiceguides.chambers.com/practice-guides/crisis-management-2026/usa/trends-and-developments

Cybersecurity and Infrastructure Security Agency (CISA). "Emergency Communications Guidance Documents and Publications." U.S. Department of Homeland Security. https://www.cisa.gov/topics/emergency-communications/emergency-communications-planning/guidance-documents-and-publications

European Commission, Directorate-General for Research and Innovation, on behalf of the Scientific Advice Mechanism (SAM) / SAPEA. "Artificial Intelligence Has Potential to Improve Emergency and Crisis Management, But Struggles to Interpret Complex Situations." December 11, 2025. https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/artificial-intelligence-has-potential-improve-emergency-and-crisis-management-struggles-interpret-2025-12-11_en

Federal Emergency Management Agency (FEMA). "National Incident Management System (NIMS) Incident Complexity Guide: Planning, Preparedness and Training." U.S. Department of Homeland Security. https://www.fema.gov/sites/default/files/documents/nims-incident-complexity-guide.pdf

Federal Emergency Management Agency (FEMA). "National Incident Management System," 3rd Edition. U.S. Department of Homeland Security, October 2017. https://training.fema.gov/emiweb/is/is700b/handouts/national_incident_management%20system_third%20edition_october_2017.pdf

Federal Emergency Management Agency (FEMA), in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA). "Planning Considerations for Cyber Incidents: Guidance for Emergency Managers." November 2023. https://www.fema.gov/sites/default/files/documents/fema_planning-considerations-cyber-incidents_2023.pdf

GS Communications. "Navigating the Storm: Applying the RACI Model to Crisis Communications." https://gscommunications.com/news/navigating-the-storm-applying-the-raci-model-to-navigate-crises

Institute for Public Relations (IPR). "IPR Publishes Updated Crisis Communications Report by Leading Crisis Expert Dr. W. Timothy Coombs." 2026. https://instituteforpr.org/updated-crisis-communications-report-w-timothy-coombs/

Roberts, P.S. "How AI Is Changing Our Approach to Disasters." RAND Corporation Commentary, August 27, 2025. https://www.rand.org/pubs/commentary/2025/08/how-ai-is-changing-our-approach-to-disasters.html

U.S. Department of Homeland Security, Science and Technology Directorate. "Feature Article: AI Means Better, Faster and More for First Responders." October 31, 2024. https://www.dhs.gov/science-and-technology/news/2024/10/31/feature-article-ai-means-better-faster-and-more-first-responders