☎ +44 1432 818999 ✉ info@initiativetraininggroup.com

Travel Risk Guidance | ISO 31030-Aligned

Designing an Emergency Response Plan People Will Actually Use

A practical white paper for organisations responsible for travelling employees

Executive Summary

Many organisations have an emergency response plan. Far fewer have one that people can find, understand, and use under pressure.

The problem is rarely a complete absence of procedure. More often the plan is too long, too complicated, or too dependent on people who may not be available when an incident occurs. Roles are unclear. Contact details are outdated. Decisions require senior approval, but nobody has defined what happens while that approval is being sought.

A usable plan helps people act in the first minutes of an incident — it doesn't just describe how the organisation believes an emergency should be managed. For organisations with travelling employees, it also has to account for distance, time zones, unfamiliar local conditions, and information that may arrive incomplete or contradictory.

An effective plan should:

- explain when and how it is activated
- identify who has authority to make decisions
- define roles in plain language
- provide immediate actions for foreseeable incidents
- establish reliable communications
- connect travellers with organisational support
- record decisions and actions
- be tested regularly
- remain short enough to use

The goal isn't to predict every possible emergency. It's to build a structure that lets the organisation respond coherently when the unexpected happens.

Contents

1. Why Emergency Plans Fail

Emergency plans tend to fail for predictable reasons. They're written to demonstrate compliance rather than support action. They contain long descriptions of policy and little practical instruction. They assume key personnel will be available, communications will work, and accurate information will arrive quickly.

Emergencies rarely show that kind of courtesy.

A travel-related incident might begin with a fragmented phone call, a missed check-in, a news report, a message from a local office, or an alert from a security provider. The organisation may not know immediately whether it involves one traveller, several, or a wider regional disruption — which means the first responders inside the organisation are likely working with limited information, competing priorities, uncertain authority, pressure from senior management, concerned relatives, operational disruption, and rapidly changing conditions, all at once.

> **The bar to clear:** a plan that can't function under those circumstances isn't an emergency response plan. It's a statement of good intentions.

2. Start With How Incidents Are Really Reported

Plans are often built on the assumption that an incident will arrive through the correct channel. In practice, information can turn up almost anywhere — a traveller calling a line manager, a family member contacting HR, a colleague posting in a messaging group, a travel management company sending an alert, or the communications team spotting it on social media before security even knows.

The plan has to account for that. Every employee who might receive an initial report should know three things:

- who must be contacted
- what information should be collected
- what must not be promised

The reporting process itself should stay simple. At minimum, the organisation needs to establish:

- who's involved
- what happened, where, and when
- whether anyone is injured or in immediate danger
- how the person reporting can be reached
- what's already been done

The person taking the report doesn't need to solve the incident — they need to capture the essentials and get them to the right decision-maker fast.

3. Define What Activates the Plan

Not every delayed flight needs a crisis team. Equally, organisations shouldn't wait until an incident is severe before activating a structured response.

The plan should set clear activation thresholds — things like:

- death or serious injury
- arrest or detention
- a missing or uncontactable traveller
- kidnapping or unlawful confinement
- a serious medical emergency
- a major security incident near a traveller
- a natural disaster affecting the itinerary
- civil unrest disrupting movement
- an evacuation or relocation requirement
- loss of critical communications
- major transport disruption affecting several travellers
- significant reputational or media interest

Activation should be based on potential impact, not just confirmed facts. An unverified report may still justify assembling the response team, checking traveller locations, and preparing options — it's far easier to scale a response down than to recover time lost through hesitation.

4. Build the Response Around Functions, Not Job Titles

Plans often assign responsibility to senior titles. That falls apart the moment the named individual is travelling, unavailable, or no longer with the organisation — and the corporate directory, that enduring monument to optimism, is rarely current either.

Responsibilities should be assigned by function instead:

- **Incident lead —** coordinates the response, sets priorities, and ensures decisions get made. Doesn't need to do every task personally; the job is to maintain control, allocate actions, and keep the team focused.
- **Traveller liaison —** maintains contact with the affected employee or group. Ideally one person acts as the main organisational contact; several departments calling independently creates confusion and adds stress.
- **Operations and logistics —** manages transport, accommodation, route changes, relocation, evacuation, and practical support, often working with local offices, travel providers, security companies, medical providers, and insurers.
- **Medical support —** coordinates clinical advice, treatment, medical evacuation, and communication with healthcare providers, while protecting the confidentiality of personal medical information.
- **Human resources and family liaison —** supports affected employees, manages welfare issues, and coordinates communication with relatives. This has to be handled carefully: information must be accurate, authorised, and consistent.
- **Communications —** manages internal messages, media enquiries, and reputational issues, and should never release information that could endanger travellers, compromise investigations, or contradict what families are being told.
- **Legal and compliance —** needed where incidents involve detention, death, data loss, regulatory reporting, contractual obligations, or liability.

- **Recorder —** maintains the incident log. This role is routinely underestimated. Without an accurate record, the organisation can't explain what information was available, why decisions were made, or whether actions were completed.

Each function needs a primary and an alternate.

5. Give People Authority Before the Incident

A plan is weakened whenever a decision needs approval from someone who can't be reached. The organisation should define delegated authority in advance — to purchase replacement travel, extend accommodation, approve emergency transport, engage medical or security providers, arrange relocation, release emergency funds, suspend travel, contact relatives, notify insurers, and approve external communications.

> **Set realistic limits:** there's little value in letting an incident manager approve £500 when the only available emergency flight costs £3,000. The response team needs to know exactly what can be authorised immediately and what requires escalation.

Good governance isn't about preventing people from acting. It's about setting clear boundaries within which they can act responsibly.

6. Separate the Plan Into Three Levels

One document shouldn't try to serve every purpose. A usable system generally needs three layers.

- **Level one: immediate action cards —** short instructions for the first person receiving a report and the initial response team — what must be done now, who must be contacted, what information is needed, and what immediate risks must be controlled. These might cover medical emergencies, arrest, missing travellers, civil unrest, natural disasters, and serious security incidents. Each card should fit on one or two pages.
- **Level two: response framework —** the main emergency response plan — activation, command arrangements, roles, communications, decision-making, escalation, and closure. It should stay concise and usable by someone who hasn't memorised it.
- **Level three: supporting information —** detailed reference material sits outside the main plan — provider contracts, insurance details, country information, contact directories, family liaison guidance, media protocols, evacuation suppliers, forms and templates, legal guidance, and business continuity arrangements.

Separating these layers stops the main plan from getting buried under material that's important but not immediately needed.

7. Design the Plan for Pressure

People read differently in an emergency. They scan rather than study, hunting for actions, names, and numbers — dense paragraphs become obstacles.

The plan should lean on:

- short sections and clear headings
- numbered actions and decision trees
- checklists, role cards, and contact tables
- simple language and consistent terminology

Critical actions shouldn't be buried inside explanatory text, and the first page should say how to activate the plan and who to contact — not open with the organisation's philosophy of resilience.

Version numbers, ownership, and review dates should be visible. Control printed copies, but not so bureaucratically that nobody can find the current version.

8. Build Communications Into the Response

Communication isn't an administrative add-on to emergency management — it's one of its central functions.

The plan should define how the organisation communicates with affected travellers, other employees in the area, senior management, families, local offices, emergency services, insurers and assistance providers, clients and partners, and the media.

Messages should be accurate, timely, and proportionate. Silence breeds anxiety and speculation; premature statements can do just as much damage. The response team should keep confirmed facts, unverified information, assumptions, decisions, and actions in progress clearly distinct — a distinction that should also show up in the incident log.

Templates help, particularly for internal alerts, traveller welfare messages, family contact records, and initial holding statements — but they should guide communication, not turn it into something robotic during a human crisis.

9. Plan for Communication Failure

Travel emergencies often happen where normal communications are already degraded — mobile networks overloaded, internet interrupted, devices lost, confiscated, or out of power.

The plan needs alternatives:

- SMS, messaging apps, email
- satellite communications
- hotel landlines and local office contacts
- travel provider messages
- scheduled check-in times and pre-agreed rendezvous points

Travellers should know what to do when they can't reach the organisation — for some journeys, that might mean moving to a nominated safe location, contacting a local partner, or attempting contact at agreed intervals.

> **Not much of a plan:** a communications plan that depends on one phone number and one mobile network isn't much of a plan.

10. Connect Emergency Response With Traveller Tracking

The organisation can't support people it can't locate. Tracking doesn't need to become intrusive surveillance — it needs to give a reasonable picture of who's travelling, where they're expected to be, and how to reach them.

At minimum, hold:

- traveller name and contact details
- itinerary and accommodation
- transport arrangements
- emergency contact
- relevant assistance and insurance details

Capture changes too. A traveller who switches hotels, extends a trip, or books transport independently can unintentionally create a gap in the organisation's response capability, so the process needs to be practical enough that travellers will actually keep it updated.

11. Include the Traveller in the Plan

Emergency response shouldn't exist only at headquarters. Travellers need to understand:

- how to request help
- what information to provide
- when to contact local emergency services
- how to protect themselves while waiting for support
- what the organisation can and can't provide
- how family communication will be handled
- what to do if communications fail

This belongs in pre-travel preparation and should stay available during the journey — and it should be concise. Someone facing a medical emergency doesn't need the full corporate response manual. They need a number to call and clear instructions.

12. Prepare for Foreseeable Scenarios

The organisation can't predict every emergency, but it can prepare for the recurring categories:

- **Medical emergency —** emergency services, medical assistance, insurance notification, hospital liaison, family communication.
- **Missing traveller —** when a missed communication becomes a concern, what checks are required, and when to escalate to local authorities or specialist support.
- **Arrest or detention —** legal support, consular contact, communication protocols, and clear limits on promises or public statements.
- **Civil unrest —** sheltering in place, route changes, relocation, communications, suspension of movement.
- **Natural disaster —** accounting for travellers, checking medical needs, confirming accommodation safety, arranging relocation, coordinating departure.
- **Violent incident or terrorism —** life safety comes first; travellers may need to run, hide, communicate only when safe, and follow local emergency instructions.
- **Evacuation —** who has authority to order movement, what triggers the decision, where people move to, and how transport is secured.

These procedures shouldn't try to script every action. They should give people a reliable starting point.

13. Record Decisions Properly

The incident log should start as soon as the plan is activated, recording:

- time and date
- information received and its source
- decisions made and why
- actions allocated and who's responsible
- completion status

- communications issued
- outstanding concerns

The log keeps things continuous when personnel change during a long incident, helps the organisation review its response and meet legal or regulatory obligations, and supports decisions if they're later questioned.

> **Facts, not commentary:** people should record facts — not speculation or personal commentary.

14. Exercise the Plan

An untested plan is an assumption. Exercises reveal problems that document reviews rarely catch — contact numbers that fail, roles that overlap, senior managers who interrupt the response structure, people who discover they lack access to the systems or authority they need.

Testing should include:

- contact checks and call-out exercises
- tabletop scenarios and communication drills
- traveller welfare exercises
- provider coordination
- full simulations where justified

Keep exercises realistic but manageable — a traveller hospitalised after a road accident abroad is a good first scenario, testing notification, medical assistance, family liaison, insurance, decision-making, and record-keeping without theatrical chaos.

The purpose is to improve performance, not catch people out.

15. Learn After Every Incident and Exercise

Every activation should end with a structured review: what worked, what caused delay, where information was missing, whether responsibilities were clear, whether providers performed as expected, whether travellers understood the process, and what needs to change.

Actions should be assigned, tracked, and completed.

> **Lessons observed vs. lessons learned:** lessons that stay inside a meeting note aren't lessons learned — they're lessons observed and then politely abandoned.

16. Keep the Plan Current

Emergency response plans deteriorate quickly. People leave, suppliers change, phone numbers are replaced, business activities expand, travel patterns shift, risks evolve.

The plan needs a named owner and a defined review cycle — contact information checked quarterly, the full plan reviewed at least annually and after any significant incident, exercise, or organisational change. Travel risk arrangements should also be revisited when the organisation enters new markets, increases travel to higher-risk destinations, or changes assistance providers.

17. Ten Tests of a Usable Plan

An organisation can assess its plan with ten direct questions:

- ☐ Can an employee find the plan quickly?
- ☐ Is the activation process clear?

- ☐ Can the first person receiving a report identify what to do?
- ☐ Are primary and alternate role-holders named?
- ☐ Can urgent expenditure be approved without delay?
- ☐ Can the organisation locate affected travellers?
- ☐ Are communication methods defined?
- ☐ Are immediate action procedures available?
- ☐ Has the plan been tested within the last year?
- ☐ Have identified improvements been completed?

If several of these come back "no," the plan is unlikely to perform in a real incident.

18. A Practical Implementation Approach

Organisations developing or revising a plan should avoid starting with a blank document. The better approach is to examine how the organisation currently manages incidents:

1. identify existing reporting routes
2. map decision-making authority
3. review available travel information
4. examine provider and insurance arrangements
5. define foreseeable incident scenarios
6. agree response roles
7. produce immediate action cards
8. develop the core response framework
9. train relevant personnel
10. test the plan
11. correct identified gaps

This process should involve the people expected to use the plan. A document designed in isolation by one department may be technically impressive and operationally useless.

Conclusion

An emergency response plan has to work when people are under pressure, information is incomplete, and normal arrangements are failing. Its value doesn't lie in the number of pages it contains — it lies in whether people understand how to activate it, know what authority they have, and can take the right actions quickly.

The strongest plans are concise, accessible, tested, and supported by trained people. They don't try to predict every emergency. They create a dependable structure for managing uncertainty.

ISO 31030 encourages organisations to integrate emergency response into a wider travel risk management system — preparing travellers, monitoring journeys, maintaining reliable support arrangements, and learning from incidents.

Initiative Training Group helps organisations review, design, and exercise emergency response arrangements that are practical, proportionate, and aligned with the realities of corporate travel.

Because an emergency plan shouldn't merely exist. It should work.