INITIATIVE
TRAINING GROUP

ISO 31030

A Plain English Summary

Travel Risk Management — Guidance for Organisations

Initiative Training Group | Hereford, United Kingdom

ISO 31030:2021,* Travel risk management — Guidance for organisations*, is the international standard for travel risk management. It gives organisations a structured way to protect people travelling on their behalf and to manage the wider risks that work-related travel can create.

Before ISO 31030, many organisations viewed travel as little more than arranging flights, hotels, and insurance. The standard adopts a broader and more serious approach, recognising that work-related travel can expose people and organisations to security threats, health issues, accidents, extreme weather, political instability, cybercrime, and disruption.

Three things are worth knowing at the outset:

- **It is guidance, not law.** No organisation is legally required to adopt it, and there is no certificate to hang on the wall — ISO 31030 is a guidance standard, so organisations cannot be certified against it. What it offers is a recognised benchmark for doing travel risk management properly.
- **It is built on ISO 31000**, the international standard for risk management, so it uses the same logic: understand the context, assess the risks, treat them, communicate, and keep reviewing.
- **It is scalable.** It can be applied by businesses, charities, government bodies, schools, and universities, and adapted to the organisation's size, activities, destinations, and level of exposure.

1. The Main Principle: Duty of Care

At the heart of ISO 31030 is the organisation's responsibility to take reasonable steps to protect people travelling for work.

This is commonly described as a **duty of care**. It means the organisation should identify foreseeable dangers, assess the risks, and put sensible precautions in place.

An organisation may use travel agents, insurers, medical assistance companies, or security providers, but it cannot simply hand over all responsibility. It must satisfy itself that its suppliers are suitable, that responsibilities are clearly understood and that appropriate arrangements are in place.

Senior management should visibly support the travel risk programme, provide adequate resources, and make it clear who is responsible for decisions. Travel safety should not be treated as an administrative task buried somewhere between expenses and photocopier maintenance.

2. Build a Programme, Not Just a Process

ISO 31030 expects travel risk management to exist at two levels: the **program** (how the organisation manages travel risk in general) and the **journey** (how each trip is assessed and supported). Many organisations do the second without the first. The standard asks for both.

A travel risk management programme should include:

- **A travel risk policy**, stating what the organisation will and will not accept, endorsed by senior management.
- **A defined risk appetite and approval thresholds** — for example, which destinations require enhanced assessment, and who is authorised to approve higher-risk travel.

- **Clear roles and responsibilities** across the organisation (see section 6).
- **Competent people**, with training appropriate to their role in the programme.
- **Verified insurance and assistance arrangements**, checked to confirm they cover the travellers, destinations, and activities in question — not merely assumed to.
- **Incident and crisis management plans** that connect travel incidents to the organisation's wider emergency arrangements, including family liaison.
- **A cycle of review**, so the programme itself is tested, audited, and improved — not just individual trips.

With that foundation in place, each journey can then be managed proportionately.

3. Preparing Before Travel

Good travel risk management begins before the traveller leaves home. The amount of preparation should reflect the level of risk involved.

Understand the destination.

The organisation should obtain reliable, current information about the destination, covering areas such as:

- Crime, personal security, terrorism, and political unrest.
- Health risks and access to medical care.
- Extreme weather and natural hazards.
- Road safety and local transport.
- Entry requirements, local laws, and cultural expectations.
- Communications, connectivity, and cyber risks.

A routine visit to a familiar, low-risk city will not require the same preparation as travel to a remote or unstable location.

Understand the traveller.

The same journey can present different risks to different people. Where relevant to the trip, the organisation should consider personal circumstances such as:

- Health conditions, medication, disability, or mobility requirements.
- Age and pregnancy.
- Gender, gender identity, or sexual orientation.
- Religion, ethnicity, or nationality.
- Language ability and previous travel experience.
- The traveller's role or public profile.

This information must be handled sensitively, confidentially and in line with data protection law. The purpose is not to judge the traveller, and never to exclude anyone by default — it is to identify support they may need.

Assess the whole journey.

The organisation should consider the entire itinerary rather than looking only at the destination country. Airports, border crossings, road transfers, accommodation, working locations, and leisure time connected with the trip can all introduce additional risks.

The assessment should lead to practical decisions: whether the journey can proceed, what precautions are needed, and who has authority to approve it under the thresholds set by the programme.

Select suitable accommodation and transport.

Hotels and transport providers should be selected with safety and security in mind, not simply price, convenience, or star rating. Depending on the risk level, this may mean considering the hotel's location, fire and emergency arrangements, access control, and the reliability of transport between airport, hotel, and workplace.

For higher-risk destinations, independent checks or specialist advice may be appropriate. A polished lobby and an ambitious number of decorative cushions are not evidence of a secure hotel.

Protect information as well as people.

Travel exposes devices and data, not just travellers. Depending on the destination, precautions may include clean or loaner devices, secure connections, limiting what information travels at all, and awareness of surveillance, border inspection, and theft risks.

Brief and train the traveller.

Travellers should receive information relevant to their journey — anything from a short briefing for routine travel to specialist training for difficult environments. The traveller should understand the main risks and how to reduce them, local laws and customs, emergency contacts, and reporting procedures, what to do during a serious incident, and their own responsibilities while travelling.

Crucially, the traveller should also be able to raise concerns — or decline travel — where serious safety, health or security issues have not been properly addressed, without fear of penalty.

4. Supporting the Traveller During the Trip

The organisation's responsibilities continue while the person is travelling.

Maintain communication.

The organisation should have a reliable way to communicate with the traveller. It should know the planned itinerary, how to make contact, and who acts if contact is lost.

For some journeys this may involve confirmed travel details and scheduled contact. Higher-risk travel may require regular check-ins or a traveller-location system. Any tracking must be lawful,

proportionate, and explained to the traveller. The purpose is to provide assistance during an incident, not to inspect whether somebody ordered room service at an unreasonable hour.

Provide emergency assistance.

Travellers should know exactly whom to contact if something goes wrong, and that contact should lead somewhere useful. Appropriate support may include medical and security assistance, help replacing lost documents, support following arrest or detention, evacuation or relocation, and crisis management with family liaison.

For international or higher-risk travel, this will often mean access to assistance at any hour. Smaller organisations may provide this through an insurer or specialist assistance company rather than maintaining their own operations centre — which is entirely acceptable, provided the arrangement has been checked and travellers know how to use it.

Monitor changing conditions.

Risks can change after a journey has started. The organisation should monitor relevant developments — severe weather, transport disruption, disease outbreaks, protests, security incidents, sudden changes to entry requirements — and warn travellers when necessary.

There should be a clear process for deciding whether to change an itinerary, move the traveller, cancel an activity, or bring the traveller home, and clear authority to make that call quickly.

5. Reviewing the Trip Afterwards

Travel risk management should not end when the traveller returns.

Gather feedback.

Travellers should have an effortless way to report incidents and near misses, problems with hotels or transport, inaccurate information, health or welfare concerns, and arrangements that worked well.

The organisation should use this information to improve future assessments, briefings, suppliers, and procedures. Near misses are particularly valuable because they expose weaknesses before somebody is seriously harmed.

Provide post-travel support.

Some journeys require follow-up after the traveller returns: medical advice following exposure to illness, monitoring for delayed-onset symptoms, psychological support following a traumatic incident, or a formal debrief after higher-risk travel.

Post-travel health monitoring is not necessary after every journey. It should be based on the destination, activities, exposure, and competent medical advice.

Review the program, not just the trip.

Lessons from individual journeys should feed back into the programme: updated assessments, better briefings, revised supplier lists, adjusted thresholds. Periodically, the programme itself should be

tested — through exercises, audits, or management review — to confirm it still works and still matches how the organisation travels.

6. Who Is Responsible?

ISO 31030 makes clear that travel risk management is not the responsibility of one department alone. Depending on the organisation, those involved may include:

- **Senior management**, providing direction, authority, and resources.
- **Human resources**, supporting traveller welfare and employment responsibilities.
- **Security personnel**, assessing threats and protective measures.
- **Health and safety or occupational health**, managing medical and workplace risks.
- **Travel managers**, controlling bookings, itineraries, and suppliers.
- **IT teams**, protecting devices, information, and communications.
- **Legal and compliance teams**, advising on legal and regulatory obligations.
- **Procurement**, checking that suppliers are suitable.
- **Line managers**, approving travel and supporting their staff.
- **Travellers**, following instructions, reporting changes, and behaving responsibly.

Responsibilities should be clearly allocated, and everyone should understand what they are expected to do before, during and after travel.

7. Why Follow ISO 31030?

Organisations are not normally required by law to adopt ISO 31030. Even so, the standard provides a recognised framework for demonstrating that travel risks are being managed systematically and responsibly.

Following the guidance can help an organisation reduce injuries, illness and security incidents; meet its legal, moral and contractual responsibilities; make more consistent travel decisions; respond more effectively during emergencies; protect operations and reputation; select and manage suppliers more carefully; give travellers greater confidence; and learn from incidents so the same problem does not happen twice.

If an incident leads to legal action or regulatory scrutiny, an organisation may need to show that it took reasonable precautions. A documented, ISO 31030-aligned approach is convincing evidence of a structured and informed programme — although following the standard does not automatically remove liability, and nothing in it replaces legal advice.

In Simple Terms

ISO 31030 asks organisations to do five things:

Understand the journey. Understand the traveller. Prepare properly. Provide support. Learn from experience.

It does not expect every organisation to build an expensive security department or treat every business trip as a military operation. It expects organisations to think ahead, make informed decisions, and provide protection proportionate to the risks faced.

That is the real purpose of ISO 31030: making sure that people travelling for work are never left to manage serious and foreseeable risks alone.