INSIGHT PAPER / CORPORATE TRAVEL SECURITY & DUTY OF CARE

Beyond the Travel Brief

The New Minimum Standard for Corporate Travel Security

From checkbox compliance to accountable, intelligence-led protection of employees travelling on business

CENTRAL ASSESSMENT

A travel policy does not demonstrate that a traveller was protected. Before an employee is exposed to foreseeable overseas risk, the organisation should be able to show that threats were identified, individual exposure assessed, controls applied, residual risk accepted and the traveller prepared to act when the system fails.

Travel Risk | Duty of Care | Situational Awareness | Technology | Crisis Preparedness

EXECUTIVE ASSESSMENT

Executive Summary

International business travel is too often treated as an administrative process rather than a security decision. A booking is approved, insurance is confirmed, a country advisory is attached, an online course is acknowledged and the compliance boxes are ticked. The organisation can demonstrate that a process occurred. It cannot necessarily demonstrate that anyone genuinely assessed whether the employee was safe.

THE QUESTION THAT MATTERS **If one of your employees were seriously injured, detained or killed overseas tomorrow, could the company demonstrate why it considered sending that particular employee to that particular location on that particular day to be reasonable?**

That question is the foundation of credible travel risk management. The answer should not depend on a generic country rating or on the employee having signed a form. It should rest on a defensible chain of decisions: foreseeable threats identified, the traveller's actual exposure assessed, proportionate controls implemented, emergency arrangements established, residual risk understood and an authorised person consciously accepting what remains.

ISO 31030:2021 provides an international framework for travel risk management and specifically addresses policy, threat and hazard identification, risk assessment, prevention and mitigation. It is built on the broader principles of ISO 31000, which place risk management inside governance and decision-making rather than treating it as a stand-alone compliance exercise. [1][2][3]

For New Zealand organisations, the underlying principle is equally clear. WorkSafe states that a business must ensure, so far as is reasonably practicable, the health and safety of workers, and that work-generated risks should be eliminated or minimised. It also explicitly cautions that having large amounts of paperwork does not equal good health and safety. [4][5] That distinction goes directly to the problem this paper addresses: documentation should evidence risk management; it should never substitute for it.

No contract, meeting, sale, bid or commercial opportunity is worth the avoidable loss of an employee's life. Business can involve risk and overseas travel cannot be made risk-free. The reasonable objective is therefore not zero risk. It is informed, proportionate and accountable risk management that gives the traveller the best practicable chance of avoiding an incident, recognising deterioration early and responding effectively when prevention fails.

1. The Core Proposition

This paper proposes a practical minimum standard for organisations that send staff overseas. It is not presented as a universal legal test and it does not replace jurisdiction-specific advice. It is a professional benchmark: the minimum set of actions an organisation should be able to demonstrate when travel exposes an employee to credible security, health, information or operational risk.

CENTRAL ASSESSMENT **Compliance is not the same as protection. A credible programme must prove that risk was understood and managed, not merely that the traveller completed the required process.**

2. The Checkbox Problem

The weakness in many travel-security programmes is not the absence of policy. It is the assumption that policy completion equals risk control. The traveller receives an automated briefing, clicks through a learning module, confirms emergency contact details and obtains managerial approval. Every item may be useful. The failure occurs when those items become the objective rather than tools supporting an actual decision about exposure.

A completed checklist can show that someone was told that crime exists in a city. It cannot show whether the employee will arrive alone after midnight, whether the hotel is in an area affected by current demonstrations, whether the meeting requires carrying commercially sensitive data, whether local authorities have recently increased scrutiny of the traveller's sector, or whether the individual's nationality, gender, role, public profile, health or personal circumstances materially change the risk. These are not administrative details. They determine exposure.

The most dangerous form of compliance is retrospective comfort: a file that appears complete after an incident but contains no evidence that the real threat was examined. A policy may require a 'country risk assessment' while nobody asks whether the destination city, route, facility, meeting, timing and traveller profile create a materially different situation. The process is technically complete and operationally shallow.

NEW ZEALAND CONTEXT WorkSafe's risk-management guidance states that widely used controls are not automatically sufficient and that organisations should focus on the most effective controls for their circumstances. It also says that paperwork is not a substitute for good processes and control measures. [5]

This is why a traveller's signature should never become a mechanism for transferring organisational responsibility. The traveller has responsibilities: provide accurate information, follow reasonable controls, report concerns and make sound decisions. But where the organisation requires or directs the journey, the organisational decision to expose the employee to the residual risk must remain visible and owned.

The Employee Accepts the Assignment; the Organisation Accepts the Decision

The phrase should not be read as removing personal responsibility from the traveller. It makes a narrower point: an employer cannot treat acknowledgement as risk acceptance. If the organisation has assessed a journey as elevated risk, management should be able to identify who approved it, what controls made the trip acceptable and what circumstances would cause that approval to be withdrawn.

This matters commercially as well as ethically. A well-run travel security programme supports business because it creates clear thresholds. Managers do not need to guess whether a trip is acceptable. Travellers are not left to decide alone whether conditions have deteriorated too far. Security teams can focus resources on journeys where consequence and exposure justify additional controls. The result should be less bureaucracy for low-risk travel and more deliberate management where it matters.

MINIMUM TEST **Can the organisation explain, in plain language and with evidence, why this trip was reasonable, what could go wrong, what was done about it and who accepted the remaining risk?**

3. Travel Risk Has Changed - and Country Ratings Are Not Enough

Traditional travel security concentrated heavily on terrorism, violent crime, kidnap and medical emergencies. Those threats remain relevant, but modern business travel now routinely intersects with a wider set of exposures: civil disorder, arbitrary or unexpected detention, regulatory enforcement, hostile-state attention, industrial espionage, device compromise, cyber-enabled theft, transport failure, natural hazards, infectious disease, political disruption, reputational targeting and rapidly changing entry or immigration rules. ISO 31030 reflects this broader view by treating travel risk as a combination of safety, security, health, information and organisational consequences. [1][2]

The central analytical change is to separate destination risk from traveller exposure. Two employees can travel to the same hotel in the same city on the same day and face different risks. A junior technician carrying no sensitive information may have a relatively ordinary profile. A senior executive negotiating a politically sensitive acquisition, a researcher carrying valuable intellectual property, or an employee whose nationality or public role attracts attention may face a different threat picture without moving a single kilometre.

WORKING MODEL **COUNTRY + CITY + JOURNEY + ACTIVITY + TRAVELLER PROFILE + INFORMATION EXPOSURE + CURRENT CONDITIONS = ACTUAL TRAVEL RISK**

NPSA guidance on overseas business specifically notes that personnel may be more vulnerable in unfamiliar environments and can be targeted for information, manipulation, device tampering, crime or other hostile activity. It also stresses that protective measures should be tailored to the specific scenario rather than applied as a one-size-fits-all package. [6][7]

Risk Begins Before the Aircraft Departs

A credible assessment starts with necessity. Does the employee need to travel, does that person need to be the traveller, does the timing need to be fixed, and can the activity be performed in a safer location or remotely? This is not an argument against travel. It is the first control in any serious risk process: do not create an exposure that produces little business value.

Where travel is justified, the assessment should examine the entire journey rather than the destination label. Airport arrival time, road transport, hotel location, meeting venue, local partner, public profile, communications, access to medical care and the employee's ability to operate independently can all matter. A high-quality country brief that ignores the last kilometre of the journey can still fail the traveller.

Health Is Part of Security

The traveller's health profile and access to appropriate care should be considered alongside conventional security threats. The CDC's 2026 Yellow Book advises that international business travellers should be counselled according to the duration, frequency, destination and reason for travel. [9] The practical implication is straightforward: a traveller going repeatedly to a remote industrial site may require a different medical and evacuation plan from a colleague attending a two-day conference in a major capital.

The correct output is not a dramatic risk label. It is a clear statement of what matters for this journey, what controls are required and what conditions would make the trip no longer acceptable.

A DEFENSIBLE MINIMUM

4. The Minimum Standard for Corporate Travel Security

The minimum standard should be deliberately simple. Organisations do not need a complicated security bureaucracy for every trip. They do need a repeatable process that scales controls to credible risk and creates a record of the decisions that matter. The following eight requirements form the minimum professional benchmark proposed in this paper.

1. CURRENT THREAT ASSESSMENT

Use current, credible information for the destination, route and planned activity. Country-level advice is a starting point, not the final assessment.

2. TRAVELLER-SPECIFIC EXPOSURE

Consider nationality, role, public profile, experience, health, gender where relevant, language, access to sensitive information and other factors that materially change exposure.

3. NECESSITY AND ALTERNATIVES

Confirm the business need, timing and person. Consider whether the objective can be achieved remotely, later or in a safer location.

4. PROPORTIONATE CONTROLS

Apply controls matched to the risk: vetted transport, accommodation, information-security measures, medical arrangements, local support, movement restrictions or protective services where justified.

5. TRAVELLER PREPARATION

Give the employee a concise, trip-specific briefing and simple actions. The traveller should understand what matters, not merely receive information.

6. EMERGENCY AND COMMUNICATIONS PLAN

Define assistance routes, check-ins, medical response, crisis contacts and phone-down contingencies. The plan must still function when normal communications do not.

7. RESIDUAL RISK AND APPROVAL

Record what risk remains after controls and require approval at a level appropriate to the consequence and exposure. Elevated risk should never be approved by inertia.

8. CONTINUOUS REVIEW

Monitor material changes while the employee is travelling. Alerts matter only if there is a defined decision process for changing movement, relocating, postponing or evacuating.

The Decision Chain

The important feature is ownership. Each stage has an output that can be explained: the threat, the traveller's exposure, the controls, the residual risk and the decision. Monitoring then loops back into the process when conditions change. This is what turns a pre-travel form into a living risk-management system.

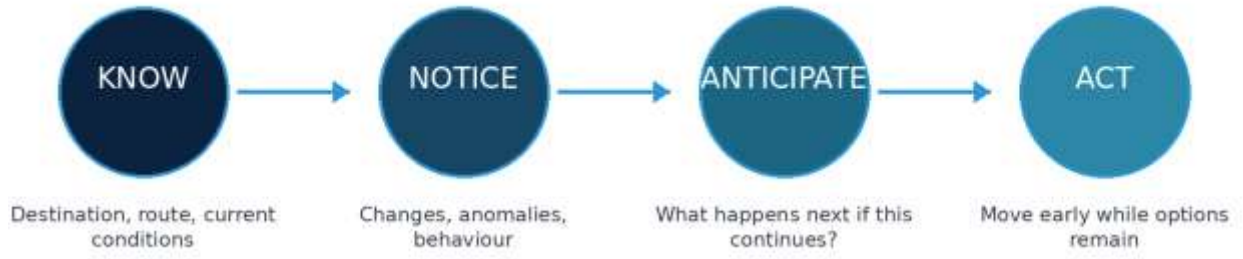
PRINCIPLE **Higher risk does not automatically mean 'do not travel'. It means more deliberate controls, clearer authority and a lower tolerance for ambiguity.**

5. Situational Awareness Without Fear

Corporate security programmes often make one of two mistakes. They provide so little information that the traveller is effectively on their own, or they overwhelm the employee with threat detail that is impossible to retain. The objective should be neither ignorance nor anxiety. It should be calm situational awareness: enough understanding to recognise change early and enough confidence to act before options disappear.

KEY IDEA **Situational awareness is not about expecting something bad to happen. It is about noticing change early enough that you still have choices.**

Experienced security professionals conduct many assessments almost subconsciously. They notice the neighbourhood, arrival time, exits, transport, crowd behaviour, changes in police presence, whether someone appears repeatedly, whether a route feels normal and whether the local environment matches what they expected. The average employee may have none of that professional conditioning. The solution is not to turn every traveller into a security officer. It is to teach a small number of repeatable habits.



KNOW means doing the small amount of preparation that changes outcomes: where you are going, how you are getting there, what is currently happening and who can help. NOTICE means paying attention to changes rather than staring at a phone while moving through an unfamiliar environment. ANTICIPATE means asking a simple question - if this continues, what happens next? ACT means moving early: leave, change route, return to the hotel, delay the meeting or call for support while those choices remain easy.

Familiarity Is Not the Same as Safety

Frequent travellers present a paradox. Experience creates useful judgement, but successful travel can also erode discipline. The first visit to a country may involve careful research, arranged transport and close attention to local conditions. By the twentieth visit, the traveller may walk out of the airport, connect to public Wi-Fi, enter the first available vehicle and assume the environment is unchanged. Nothing necessarily became safer. The traveller simply became comfortable.

The same principle applies inside countries. A person may live securely for years in one city, speak the language and understand the culture, yet still face different local risks when travelling to another province or region. A security professional will usually refresh the assessment instinctively. An ordinary employee needs a simple process that creates the same pause before movement.

COMPLACENCY TRAP **Every uneventful journey can reinforce the belief that precautions were unnecessary. In reality, good preparation may be part of the reason nothing happened - and sometimes the traveller was simply fortunate.**

6. Real-Time Situational Awareness and the Connected Traveller

Technology has transformed what a corporate travel-security programme can see and do. Modern commercial platforms and in-house systems can combine itineraries, threat intelligence, mapping, employee check-ins, geofenced alerts, emergency communications and traveller-assistance functions. Used properly, these tools can move an organisation from periodic country briefings to near-real-time awareness of who may be exposed to a developing event.

The most valuable capability is not simply tracking a dot on a map. It is connecting a material change in the environment to a decision. If a protest begins near a hotel, severe weather closes the planned route, an incident occurs near a meeting venue or authorities impose sudden movement restrictions, the system should help answer four questions quickly: Who may be affected? What does the change mean? What action is required? Who has authority to make that decision?

Capabilities That Matter

A mature system should be capable, at a level proportionate to the organisation's risk profile, of maintaining accurate traveller itineraries, pushing location-relevant alerts, requesting and recording welfare check-ins, establishing two-way crisis communication, identifying employees potentially inside an affected area, escalating missed responses and preserving an auditable record of actions. For higher-risk travel, more precise location data, dedicated monitoring and alternate communications may be justified. For routine travel, itinerary awareness and event-triggered check-ins may be enough.

TECHNOLOGY PRINCIPLE **Buy or build capability against the risk requirement. Do not mistake the possession of a platform for the existence of a travel-security programme.**

Track the Risk, Not the Employee

Location technology creates a legitimate privacy problem. Safety does not justify collecting more personal information than is necessary. The organisation should define when location information is used, how precise it needs to be, who can access it, how long it is retained and when monitoring stops. Employees should understand the purpose before travel. Where privacy law applies, the organisation must also establish the appropriate lawful basis and proportionality for monitoring.

UK Information Commissioner's Office guidance is useful beyond the UK because it expresses the principle clearly: worker monitoring may support health and safety, but it must be lawful, fair, transparent and proportionate, and excessive monitoring can intrude into private life. [8] The practical security standard should therefore be risk-triggered location awareness rather than habitual surveillance.

Technology Must Reduce Decision Time

The strongest systems compress the time between warning and action. An alert that nobody owns is noise. A check-in request that does not generate escalation when unanswered is theatre. A live map that cannot trigger a transport change or welfare call is situational awareness without decision authority. Technology earns its place when it makes the organisation faster, more precise and more resilient.

PRACTICAL TEST For every technology feature, ask: what decision does this enable, who receives the information, what happens if the traveller does not respond, and what happens when the technology itself fails?

7. When the Phone Disappears

The smartphone has become the centre of modern travel. It holds the itinerary, maps, hotel address, airline information, emergency contacts, banking applications, translation tools, identity documents, corporate messaging and often the travel-security application itself. That concentration of capability is convenient. It is also a single point of failure.

HARD RULE **If the phone is the emergency plan, there is no emergency plan.**

In an incident the phone may be the first item taken from the traveller. It may be stolen, confiscated, damaged, compromised, left behind, discharged or rendered useless by network failure. The traveller may also be injured or unable to unlock it. A credible travel programme must therefore assume that its most convenient communication tool can disappear at the moment it is needed most.

WHEN THE PHONE DISAPPEARS

1	MEMORY	Know the emergency number and first action.
2	PAPER	Carry a small emergency card separately.
3	TIME	Know when a missed check-in triggers action.
4	PLACE	Know the hotel, safe location or rendezvous.
5	BACKUP	Have alternate funds, documents or comms if warranted.

Technology creates capability. Redundancy creates resilience.

The Phone-Down Protocol

The fallback should be deliberately low-tech. The traveller should know the first emergency number without opening an application and carry a small physical card containing essential contacts, the hotel or safe location and any critical instruction that cannot reasonably be memorised. The organisation should define when a missed check-in becomes an incident, who initiates escalation and what actions are taken when contact cannot be restored.

Higher-risk journeys may justify additional redundancy: a second communication method, a separate copy of essential documents, pre-agreed rendezvous points, an alternate transport provider, emergency cash or payment options, and specific detention or medical protocols. These controls should be driven by the assessment rather than turned into universal travel theatre.

Information Security Travels With the Employee

Loss of the phone is not only a welfare problem. It may be an information-security incident. NPSA guidance recommends considering what information is carried on overseas devices and, where appropriate, providing clean devices containing only the information required for the journey. [7] The principle is minimisation: if information is not needed for the trip, do not expose it to the trip.

The same logic applies after travel. Where the journey involved elevated cyber or hostile-state exposure, the return process may need to include device inspection, password changes, reporting of unusual approaches and a short security debrief. The employee who experienced something that felt insignificant may hold the first indicator of a wider organisational threat.

RESILIENCE PRINCIPLE **Technology creates capability. Redundancy creates resilience. The security plan should survive the loss of the device on which the plan is normally displayed.**

8. From Assessment to Approval

Risk assessment has little value if it does not change a decision. The organisation should define a travel risk threshold: the level of residual risk below which normal approval is sufficient and above which additional control, senior acceptance, postponement or cancellation is required. The threshold does not need to be mathematically perfect. It needs to be understood, repeatable and connected to authority.

The decision chain should be explicit: identify the threat; assess how the individual traveller is exposed; apply controls; determine the residual risk; approve, escalate, postpone or cancel; then monitor for change. If a material development occurs after approval, the decision is reopened. This is the difference between approving a trip and managing it.

The ADG Consult NZ Recommended Minimum Travel Security Standard

An organisation meeting a credible minimum standard should be able to demonstrate eight things for any journey that exceeds routine low risk: a current threat assessment; an individual exposure assessment; confirmation that the trip is necessary; controls proportionate to the risk; a concise traveller briefing; functioning emergency and communication arrangements including a phone-down fallback; a recorded residual-risk decision by an appropriate authority; and ongoing monitoring with defined triggers for reassessment.

The standard should scale. A low-risk conference visit to a stable city may require only itinerary capture, basic destination advice, emergency support information and routine monitoring. A remote industrial visit, politically sensitive negotiation or journey involving elevated crime, health, detention, information or unrest risk should require more. The purpose is not to impose executive-protection measures on ordinary business travel. It is to ensure that controls rise with credible exposure.

MANAGEMENT TEST **Before approving elevated-risk travel, the decision-maker should be able to answer: What could seriously harm this employee? Why is this person exposed? What have we done to reduce that exposure? What remains? What would make us stop the trip?**

Conclusion: Protection Must Be Real

International business depends on people crossing borders, entering unfamiliar environments and accepting a degree of uncertainty. The answer is not to create a workforce that is afraid to travel. Fear narrows judgement and undermines business. The answer is to create travellers who are informed, alert and supported by an organisation that understands its own responsibilities.

The test of a travel-security programme is therefore not the number of policies, alerts, subscriptions or forms it can produce. It is whether those systems help a real employee avoid a foreseeable threat, recognise deterioration early, obtain help quickly and continue functioning when the easiest technology fails.

A company should never discover after a serious incident that nobody had actually decided the journey was safe enough. The risk may have been visible. The controls may have been available. The warning may have existed. What was missing was ownership.

FINAL ASSESSMENT **Before an employee is sent abroad, somebody must understand the risk, somebody must reduce it and somebody with the right authority must accept responsibility for what remains. That is the minimum standard.**

No commercial opportunity is worth an avoidable loss of life. Good travel risk management does not obstruct business. It protects the people who make business possible.

SOURCE NOTES

References and Source Notes

This paper draws principally on international risk-management standards and official government guidance. The proposed ADG minimum standard is an analytical synthesis intended to support organisational policy design; it is not legal advice and should be adapted to the law, operating environment and risk profile of the organisation concerned.

[1] International Organization for Standardization (ISO). ISO 31030:2021, Travel risk management - Guidance for organizations. Published September 2021. https://www.iso.org/standard/54204.html

[2] ISO/TC 262. "ISO 31030:2021 - Managing travel risks - Guidance for organizations." Background and scope of travel risk management. https://committee.iso.org/sites/tc262/home/projects/published/iso-310302021----managing-travel.html

[3] International Organization for Standardization (ISO). ISO 31000:2018, Risk management - Guidelines. Current edition confirmed in 2023. https://committee.iso.org/standard/65694.html

[4] WorkSafe New Zealand. "What is the primary duty of care?" Guidance on the Health and Safety at Work Act 2015 and the responsibility of businesses for worker health and safety. https://www.worksafe.govt.nz/managing-health-and-safety/getting-started/understanding-the-law/primary-duty-of-care/what-is-the-primary-duty-of-care/

[5] WorkSafe New Zealand. "Reasonably practicable" and "How to manage work risks." Guidance on eliminating or minimising work-generated risks, selecting effective controls and avoiding paperwork-only approaches. https://www.worksafe.govt.nz/managing-health-and-safety/getting-started/understanding-the-law/reasonably-practicable/

[6] UK National Protective Security Authority (NPSA). "Considering the Risks." Guidance on overseas business, staff vulnerability, deliberate targeting, information extraction and device tampering. https://www.npsa.gov.uk/considering-risks

[7] UK National Protective Security Authority (NPSA). "Trusted Research - Countries and Conferences." Cyber security advice for overseas travel, including minimising data carried and use of clean devices where appropriate. https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-countries-and-conferences

[8] UK Information Commissioner's Office (ICO). "Data protection and monitoring workers." Guidance on lawful, fair, transparent and proportionate monitoring, including location-related technologies. Guidance noted by the ICO as under review following legislative changes. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/

[9] US Centers for Disease Control and Prevention. CDC Yellow Book 2026, "The International Business Traveler." Guidance on business-travel health preparation according to duration, frequency, destination and reason for travel. https://www.cdc.gov/yellow-book/hcp/travel-for-work-other/international-business-traveler.html

Editorial Note

The examples in this paper are illustrative and deliberately generic. References to travel-risk technology describe capabilities rather than endorsing any commercial provider. Risk controls should always be proportionate to a credible assessment of threat, vulnerability and consequence.

ADG CONSULT NZ Insight Papers are designed to challenge established security assumptions and translate risk analysis into practical organisational decisions.