

A collage of black and white images is arranged diagonally across the page. It includes a close-up of a car's interior, a view of skyscrapers with an airplane in the sky, a hand holding a pen over documents, and a group of people in business attire in a meeting. The central text is set against a dark, diamond-shaped background.

Client-Facing ISO 31030 Travel Risk Management Audit Checklist

Dubai, UAE
+971 4 363 5392
www.sicurogroup.com

Client-Facing ISO 31030 Travel Risk Management Audit Checklist

This simplified checklist is designed to help organizations audit their travel risk management program against ISO 31030:2021 - not just for compliance, but for operational credibility.

While the original ISO framework follows a Plan–Do–Check–Act structure, most audit tools stop at documentation. This one does not.

Sicuro Group has long challenged the travel-risk industry's dependence on obsolete tech, bloated vendor models and generic toolkits. Instead, we advocate for decentralised, transparent solutions that are field-tested, cost-conscious, and adaptable to your real operating environment:

- Use what already works (e.g. WhatsApp, SMS, Teams)
- Build trust-based local partnerships with proven capability
- Focus on consequence-led risk assessments—not coverage area optics

The checklist below preserves ISO 31030's structure but translates it into precise, actionable guidance. It reflects what we've seen work under pressure, and what clients need to protect their people while making smart, risk-aligned decisions.

This enhanced checklist combines the foundational ISO 31030:2021 standard with real-world insights from operational experience across fragile and high-risk environments. It is designed not just for compliance, but for practical risk reduction and decision confidence. Each section includes original ISO criteria, audit evidence, and specific recommendations tailored for operational value.

1. Governance & Policy

1.1 Travel Risk Management Policy & Objectives

- Approved, up-to-date policy that defines scope, objectives, and duty of care. Should reflect company risk appetite, signed by leadership, and reviewed annually.
- Action: If outdated, refresh with clear thresholds and stakeholder input. Confirm that the policy has been tested in live or simulated events.

1.2 Roles, Responsibilities & Accountability

- Documented structure with clear accountability at executive level. Include security, HR, travel ops, and a designated decision-maker during crises.
- Action: Confirm if these roles are known, rehearsed, and empowered. Drill scenarios that test authority to cancel or modify travel.

1.3 Legal and Regulatory Compliance

- Register of applicable legal obligations (e.g. data protection, labour laws, insurance cover). Reviewed annually and reflected in policy.
- Action: Verify coverage against new jurisdictions and pandemic-era liability. Test response to data breach or cross-border compliance issue.

1.4 Integration with Enterprise Risk

- TRM integrated into enterprise risk register and continuity plans.
- Action: Audit if travel risks are discussed at board or executive level. Verify if key enterprise risks (e.g. cyber, geopolitics) are reflected in travel guidance.

2. Risk Planning & Authorisation

2.1 Pre-Travel Risk Assessment

- Trip-specific risk assessment documented before travel approval. High-risk travel requires escalation.
- Action: Run a spot-check on five recent trips. Were approvals based on real-time conditions, or were they rubber-stamped?

2.2 Destination Risk Ratings

- Maintain a destination risk matrix with multiple sources (gov't advisories, intelligence providers).
- Action: Audit the matrix's update cycle. Are alerts used operationally—or just for display?

2.3 Individual Risk Matching

- Traveller health, experience, and vulnerability assessed in context.
- Action: Test if high-risk profiles (e.g. first-time traveller, pre-existing condition) triggered extra precautions.

2.4 Cost vs Exposure Justification

- Apply Return on Risk logic. If travel cannot materially change outcomes, consider alternatives.
- Action: Audit if justification includes cost-benefit analysis for high-exposure trips.

3. Real-Time and In-Country Readiness

3.1 Communication & Tracking

- Comms protocol includes WhatsApp, SMS, fallback lines. GPS tracking optional.
- Action: Test 24/7 hotline. Audit when it was last activated. Evaluate comms performance during prior incidents.

3.2 Local Capability Verification

- Partners have in-country assets and SOPs—not just coverage claims.
- Action: Select three countries. Request proof of delivery capability (drivers, fixers, medevac).

3.3 Decision Ownership in Crisis

- Crisis escalation roles clearly assigned and tested.
- Action: Run a tabletop drill. Identify if middle managers can act without deferring to HQ.

4. Learning & Improvement

4.1 Post-Trip Feedback & Lessons

- Traveller debriefing process includes incident capture, stress indicators, and improvement suggestions.
- Action: Check if debriefs led to policy changes. Were insights circulated or archived?

4.2 Incident Recording & Analysis

- All incidents and near misses logged, analysed, and actioned.
- Action: Review past three months. Were corrective actions issued—and closed?

4.3 Annual Review

- TRM reviewed yearly across functions. Metrics tracked.
- Action: Validate that the review was scheduled, minuted, and led to updates.