INTERNATIONAL STANDARD

ISO 31030

First edition
2021-09

Travel risk management — Guidance for organizations

Gestion des risques liés aux voyages — Recommandations pour les organismes

Reference number
ISO 31030:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 262, *Risk management*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document is intended to assist those managing and participating in organizational travel. The management of travel risk is a component of any organization's travel-related activities and should include interaction with stakeholders.

There are many reasons why people travel for their organization. Travelling has increasingly become a common feature of people's jobs or functions. Consequently, organizations need to meet their duty of care across multiple jurisdictions in different parts of the world.

Travellers, whether international or domestic, can be faced with unfamiliar situations and environments that have different risk profiles to those of their normal location. Road accidents, disease outbreaks, epidemics and natural disasters, as well as conflict, crime (including cyber and information), cyber threats, terrorism and political and socially motivated instability, can threaten the safety, security (including information security) and health (including mental health) of travellers, and can adversely affect the outcome of their travel objectives.

NOTE Unless otherwise indicated, any reference to security also includes information security.

Managing risks for travel to a country where the organization has no local base requires more comprehensive controls than for locations where risk profiles are well known and treatments have already been established. Timeliness and accuracy of intelligence, analysis and advice, including travel warnings, are increasingly important in influencing travel decisions.

Travel risk management (TRM) requires that organizations anticipate and assess the potential for events, develop treatments and communicate anticipated risk exposures to their travellers. Advising and providing travellers with adequate medical and emergency response guidance, security and information security precautions, including challenges to travel logistics, can significantly impact the outcome of disruptive events.

This document provides a means for organizations to demonstrate that travel decisions are based on the organization's capacity to treat risk using internal resources or with external assistance. Not all travel requires the same level of rigour for risk assessment and management. Although this document provides a comprehensive set of risk treatment options that an organization can consider, application should be reasoned and proportionate to the risk exposure. This will help the organization and individual travellers realize the opportunities and benefits for which travel is required.

This document proposes that the organization's overall appetite and acceptance of risk should not take precedence, or be used exclusively, in deciding whether travel is appropriate for security, safety or health reasons.

This document is based on the principles, framework and process of ISO 31000, as illustrated in Figure 1. Travel-related risk presents a specific context and an organization's existing risk management process can be adapted to reflect this. It is also aligned with the core occupational health and safety management system set out in ISO 45001. As such, elements of this document can assist or inform organizations developing such management systems, but it is not a management system standard.

This document can be used on a standalone basis or integrated within other risk management programmes.

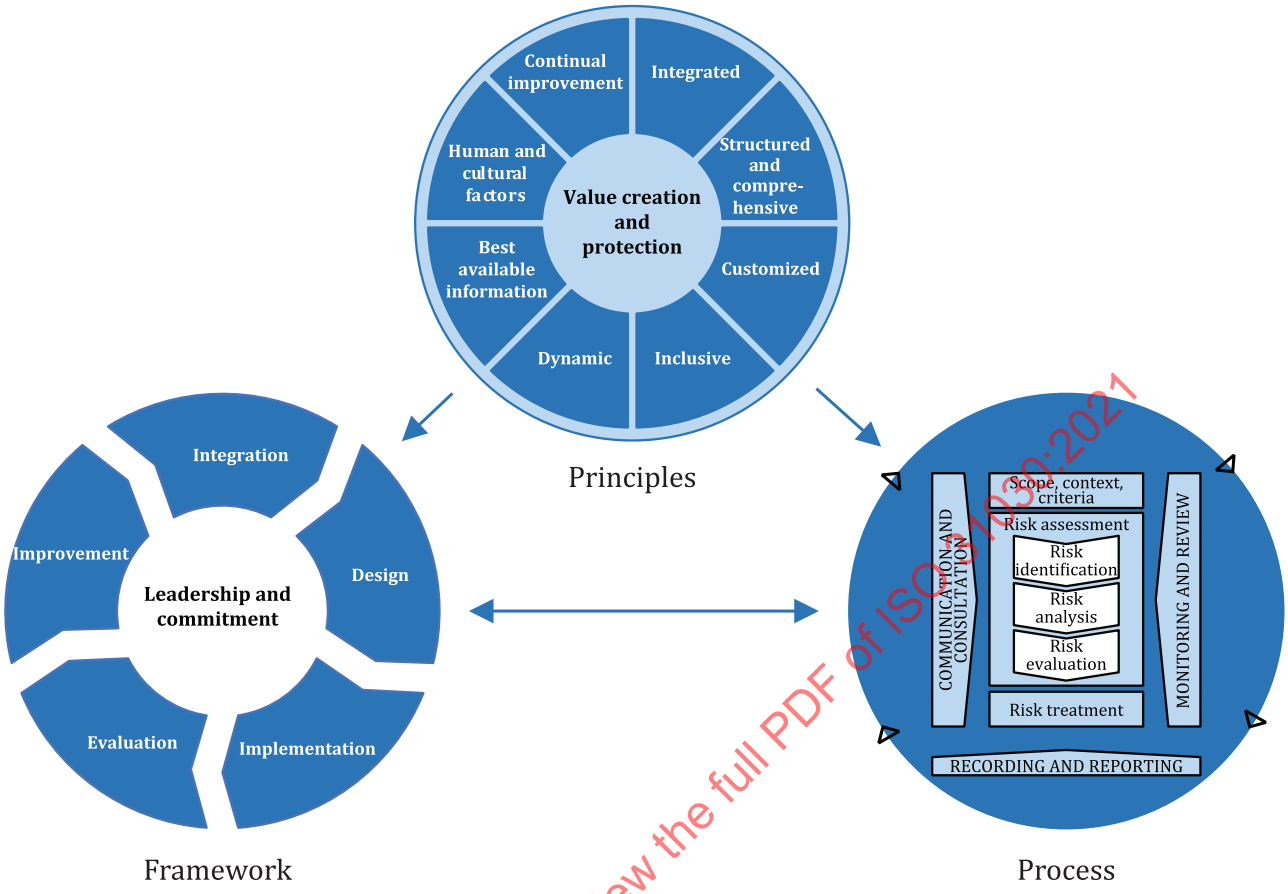

Figure 1 — Principles, framework and process

One of the aims of this document is to promote a culture where travel-related risk is taken seriously, resourced adequately, and managed effectively. And where the benefits to the organization and relevant stakeholders are recognized. Such benefits include:

— protecting personnel, data, intellectual property and assets;

— reducing legal and financial exposure;

— enabling business in high-risk locations;

— enhancing an organization's reputation and credibility, which in turn can have a positive effect on competitiveness, staff turnover and talent acquisition;

— improving worker confidence in health, safety and security arrangements with regard to travel;

— contributing to business continuity capability and organizational resilience;

— demonstrating the organization's ability to control its travel-related risks effectively and efficiently, which can also help in lowering its insurance premiums;

— providing assurance to business partners, thus banks and investors will be more willing to finance its business;

— enabling the organization to meet customers' expectations in terms of the security and stability of their supply chain;

— increasing general productivity;

— contributing to meeting the sustainable development goals by strengthening the social dimension of sustainability.

In this document, the following verbal forms are used:

a) “should” indicates a recommendation;

b) “may” indicates a permission;

c) “can” indicates a possibility or a capability.

Information marked as “NOTE” is intended to assist the understanding or use of the document.

“Notes to entry” used in Clause 3 provide additional information that supplements the terminological data and can contain provisions relating to the use of a term.

Travel risk management — Guidance for organizations

1 Scope

This document gives guidance to organizations on how to manage the risk(s), to the organization and its travellers, as a result of undertaking travel.

This document provides a structured approach to the development, implementation, evaluation and review of:

— policy;

— programme development;

— threat and hazard identification;

— opportunities and strengths;

— risk assessment;

— prevention and mitigation strategies.

This document is applicable to any type of organization, irrespective of sector or size, including but not limited to:

— commercial organizations;

— charitable and not-for-profit organizations;

— governmental organizations;

— non-governmental organizations;

— educational organizations.

This document does not apply to tourism and leisure-related travel, except in relation to travellers travelling on behalf of the organization.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
competence
ability to apply knowledge and skills to achieve intended results

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

[SOURCE: ISO 22300:2021, 3.1.42]

3.2
crisis
abnormal or extraordinary event or situation that threatens an *organization* (3.9) and requires a strategic, adaptive and timely response in order to preserve its viability and integrity

Note 1 to entry: The event can include a high degree of uncertainty.

Note 2 to entry: The event can exceed the response capacity or capability of the organization.

Note 3 to entry: Given the nature of a crisis, it is possible that there will not be an adequate or appropriate plan to deal with the event, such that a flexible and dynamic approach is needed.

3.3
crisis management team
group of individuals functionally responsible for the direction and implementation of the *organization's* (3.9) *crisis* (3.2) management capabilities

3.4
duty of care
moral responsibility or legal requirement of an *organization* (3.9) to protect the *traveller* (3.21) from *hazards* (3.5) and *threats* (3.17)

Note 1 to entry: The legal aspect of duty of care can arise from, among others, negligence, contract and statute.

Note 2 to entry: Legal requirements and how they arise, including insurance coverage, can differ between jurisdictions.

Note 3 to entry: Legal requirements can be qualified in scope (e.g. it is possible they will not be absolute).

Note 4 to entry: Organizations should seek advice from a competent legal adviser to ascertain the scope and nature of their duty of care relating to the context of this document.

3.5
hazard
source of potential harm

[SOURCE: ISO 31073:—[1)], 3.7.5, modified — Note 1 to entry has been deleted.]

3.6
incident
adverse event that can be, or can lead to, a disruption, loss, emergency or *crisis* (3.2)

Note 1 to entry: An incident can negatively impact a *traveller's* (3.21) health, safety and security.

Note 2 to entry: An incident can negatively impact the *organization* (3.9), e.g. by reputational damage, financial loss.

Note 3 to entry: An incident can negatively impact organizational resilience.

1) Under preparation. Stage at the time of publication: ISO/DIS 31073:2021.

3.7
incident management team
group of individuals functionally responsible for planning for the likelihood and management of an *incident* (3.6)

Note 1 to entry: Responsibilities of the incident management team can include liaison with external *organizations* (3.9), *stakeholders* (3.15) and families.

3.8
off-duty time
time when *travellers* (3.21) are not engaged in work activities but remain under the general supervisory responsibility of the *organization* (3.9)

Note 1 to entry: This can include a weekend depending on the trip duration.

3.9
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, association, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 31022:2020, 3.4, modified — Note 1 to entry has been modified.]

3.10
personal leave time
period of time, occurring before, after or within the scheduled duration of the work activity or project, that falls outside the supervisory responsibility of the *organization* (3.9)

3.11
provider
organization (3.9) providing services or products, or both, to the organization in accordance with agreed specifications, terms and conditions

3.12
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and *threats* (3.17).

Note 2 to entry: Objectives can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018, 3.1]

3.13
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO 31073:—, 3.6.1]

3.14
risk treatment
process to modify *risk* (3.12)

Note 1 to entry: Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— taking or increasing risk in order to pursue an opportunity;

— removing the risk source;

— changing the likelihood;

— changing the consequences;

— sharing the risk with another party or parties (including contracts and risk financing);

— retaining the risk by informed decision.

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO 31073:—, 3.10.1]

3.15
stakeholder
person or *organization* (3.9) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: The term "interested party" can be used as an alternative to "stakeholder".

[SOURCE: ISO 31000:2018, 3.3]

3.16
student
individual on placement, internship, apprenticeship or otherwise, under the control of an employing *organization* (3.9) as part of a training programme, or enrolled in a school or other educational institution

Note 1 to entry: As students can be under the age of legal responsibility, it is possible they will not be able to make legal decisions themselves.

3.17
threat
potential source of danger, harm or other undesirable outcome

[SOURCE: ISO 31073:—, 3.7.7, modified —Notes 1 and 2 to entry have been deleted.]

3.18
travel
movement of a person(s), on behalf of an *organization* (3.9), which comes within the scope of the organization's *duty of care* (3.4)

Note 1 to entry: The movement can be either domestic or international.

3.19
travel risk
effect of uncertainty on objectives due to *travel* (3.18)

3.20
travel risk management
TRM
coordinated activities to direct and control an *organization* (3.9) with regard to *travel risk* (3.19)

3.21
traveller
person(s) undertaking *travel* (3.18)

3.22
worker
person performing work or work-related activities that are under the direct or indirect control of the *organization* (3.9)

Note 1 to entry: Persons perform work or work-related activities under various arrangements, paid or unpaid, such as regularly or temporarily, intermittently or seasonally, casually or on a part-time basis.

Note 2 to entry: Workers include top management, managerial and non-managerial persons.

Note 3 to entry: The work or work-related activities performed under the control of the organization may be performed by workers employed by the organization, workers of external *providers* (3.11) (contractors, sub-providers), individuals, agency workers, and by other persons to the extent the organization shares control over their work or work-related activities, according to the context of the organization.

[SOURCE: ISO 45001:2018, 3.3, modified — "direct or indirect" has been added to the definition and "sub-providers" has been added to Note 3 to entry.]

4 Understanding the organization and its context

4.1 Operating context

4.1.1 General

It is important that an organization has a clear understanding of the factors that can affect or influence its TRM programme objectives, including the external and internal context in which it operates.

The external context can include, but is not limited to:

a) political, socio-economic, cultural, religious/ethical, legal or regulatory factors, whether international, national, regional or local;

b) political violence (including terrorism, insurgency, politically motivated unrest and war);

c) social unrest (including sectarian, communal and ethnic violence);

d) violent and petty crime;

e) the quality, availability and reliability of the modes of transport;

f) the quality, availability and reliability of telecommunications;

g) the state of industrial relations;

h) the effectiveness of public and private security and emergency services;

i) the responsibilities of other parties (e.g. clients) for the organization's travellers;

j) natural or geological factors;

k) susceptibility to natural disasters;

l) potential health hazards, including epidemics and pandemics;

m) the quality of local health infrastructure and medical care;

n) information/cyber security;

o) the quality of hotel/accommodation;

p) ground/road conditions.

The internal context can include, but is not limited to, the organization's:

— vision, mission, values and culture;

— governance, structure, roles responsibilities and accountabilities;

— strategy, objectives and policies;

— plans, standards, guidelines, regulations and instructions;

— risk management strategy and risk criteria;

— range and type of travel activities;

— capabilities, including traveller competences and profiles;

— resources, techniques and tools needed to manage organizational travel risk;

— data, information systems and information flows.

4.1.2 Industry/sector specific

The industry/sector in which an organization operates is another factor which can affect the risks faced by travellers. An organization should be aware of the relevant legislation, regulatory requirements, codes of practice, etc. which are relevant to their industry/sector in their country of origin and in other countries in which they operate. It should also take account of its duty of care, business resilience policies and arrangements and sustainability objectives, which can all have a positive effect on risk treatment considerations.

Organizations need to proactively monitor and review their identified, evolving and emerging risks. Their impact on the organization's TRM should be considered and any changes recorded and acted upon.

4.1.3 Risk profile

An organization should have a clear understanding of its risk profile and the dynamic TRM landscape in which it operates or plans to operate. To do this, an organization should review TRM objectives in relation to:

— context of the organization;

— the operational sector of the organization;

— specific operations or assignments, or both;

— destinations;

— individual traveller profiles and objectives.

A risk profile can incorporate different risks which can be interdependent.

The risk profile for travel should be reviewed regularly and after any significant change in the internal and external operational context. Results should be made known through internal and external communications.

4.2 Stakeholders

The organization should determine the internal and external stakeholders that are relevant to TRM (see Table 1).

Depending on the size of the organization and its organizational travel needs, the TRM function can be combined with other functions. Certain functions can also be supported by specialist third-party providers.

Table 1 — Example of internal and external stakeholders

Internal stakeholders (including those for functions)		**External stakeholders**
— health and safety/environment, health and safety/occupational health and safety — corporate security/information security — data privacy — business continuity — crisis management — incident management — corporate social responsibility/ sustainability — global travel/corporate travel — human resources/internal mobility/ training — regional management — risk management	— marketing and communications — board of directors — procurement and sourcing — compliance — operations — workers/students — insurance — finance — audit — legal — unions/workers council — travel and mobility — medical — security	— insurance providers — travel management companies — TRM companies — appropriate government agencies — regulators and emergency services — providers and sub-providers — clients — travellers' designated emergency contact — travellers' dependants — local partners or communities

4.3 Travelling population

Attention needs to be given to the traveller's profile in relation to destinations because factors such as race, competencies, nationality, cultural identity, gender, sexual orientation, religion, age, occupation, position, disability or medical history can all affect the risks associated with the travel. The risks can extend beyond safety and security and can also include medical and other needs.

An organization can have several different types of traveller, or group of travellers, all with varying duty of care requirements. The TRM team should liaise closely with the organization's human resources or legal department to develop a full understanding of the different types of travellers. These can include, among others:

— direct workers;

— other workers in the organization and its supply chain;

— interns and guests of the organization;

— families (and others that rely on the traveller for support, e.g. financial support) travelling with the primary traveller;

— students/pupils of universities/schools.

The pattern of travel should also be considered, for example:

— distinguishing short-term and long-term travellers (including expatriates);

— nationally based, remote workers;

— workers on rotation.

4.4 Business objectives, risk appetite and criteria

An organization should balance its business objectives and opportunities with the steps necessary to manage the risks and threats it encounters. Risk treatment options should be proportionate to the level of risk foreseen or expected. An organization should consider the level of risk it is prepared to accept to meet its business objectives and take advantage of any opportunities, while putting in place appropriate measures to manage the risk effectively and efficiently. There can be occasions where the level of risk is unacceptable and the travel should not take place.

The organization's travel risk criteria should be recorded in the TRM policy.

4.5 Travel risk management and delivery

The nature and scale of an organization's travel risk will inform how the risk is managed and delivered. The risk profile of an organization with occasional travel to low-risk locations is very different to one operating frequently in high-risk locations.

The risk profile will also inform the extent to which the organization can manage the risks using its own resources or will need to rely on support from third-party providers to assist or deliver necessary functions. This will be an important factor to address when developing and implementing a TRM policy and programme. Due consideration should be given to providing a cost–benefit analysis to aid the decision-making process. Further guidance on cost–benefit analysis can be found in IEC 31010.

5 Managing travel risk

5.1 Leadership and commitment

Top management should take and demonstrate ownership of the organization's travel risks and provide evidence of its commitment and support in their effective management by:

— taking accountability for the effectiveness of the TRM process;

— ensuring that the TRM policy and TRM objectives are established and are compatible with the strategic direction of the organization;

— ensuring the integration of TRM into the organization's business processes;

— ensuring that the resources needed for the TRM programme are available;

— communicating the importance of effective TRM and of conforming to the TRM process and its legal responsibilities;

— ensuring that the TRM programme achieves its intended outcome(s);

— directing and supporting persons to contribute to the effectiveness of the TRM programme;

— supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility;

— conducting, at planned intervals, management reviews of the TRM programme;

— promoting improvement.

An organization should provide instructions and adequate resources for the development and implementation of a travel risk programme.

5.2 Policy

The TRM policy should be a high-level document that indicates the organization's TRM strategy, which is part of its broader risk management strategy. This policy should be fully aligned with the intentions and direction of the organization, as formally expressed by its top management.

Top management should establish a TRM policy that:

— defines the overall principles, intention and direction to achieve objectives;

— is appropriate for the needs and resources of the organization;

— becomes an integral part of the organization's management policy;

— is aligned with the organization's risk management, business continuity, travel procurement and sustainability policies;

— refers to relevant legislation, standards, policies and codes of practice;

— establishes principles for the risk assessment process;

— takes into consideration (or establishes) the risk criteria of the organization;

— defines roles, responsibilities and accountabilities of all relevant stakeholders including their competence;

— sets out the organization's policy with respect to off-duty time and personal leave time (both sometimes referred to as "bleisure") associated with any travel;

— takes into consideration the multi-traveller policy and accompanying persons when relevant.

The TRM policy should:

— be approved by top management;

— be made available to all appropriate stakeholders;

— be defined and effectively communicated within the organization through information, education and training;

— be integrated with any broader risk management framework to ensure a consistent approach to risk management within the organization;

— be periodically reviewed for relevance and consistent application.

In order for an organization to be agile and responsive to organizational needs, the TRM policy should include an exception process. This should be designed to ensure that any requested exceptions to the policy requirements are:

— considered in line with the organization's risk appetite, priorities and other relevant criteria;

— elevated and approved by the relevant stakeholders;

— managed with compensating controls if necessary;

— recorded and reported.

For example, travellers sometimes need to book travel outside the TRM policy for some reason. In these cases, it's crucial that they submit a policy exception request.

It is important that the policy exception request, approval or disapproval, and any associated controls or recommendations, are acknowledged and recorded.

If the organization uses a travel management company to make travel bookings, then the policy, the policy exception process and any changes to either should be communicated to the travel management company in a clear and timely manner.

5.3 Roles, responsibilities and accountability

Ultimate accountability for risk resides with top management even where responsibilities have been delegated to others. The concept of "criminal liability" of top management can exist in certain jurisdictions. If delegation of authority is in place, it should be documented in writing.

The TRM function should be managed by a person or team with the necessary competence. This can be either in a dedicated role or with additional responsibilities.

The TRM policy should set out the responsibilities of the various internal and external stakeholders that have a role in delivery of both routine operations and non-routine situations, such as during an incident.

Subclause 4.2 provides a list of internal stakeholder functions that can have a role.

The responsibilities of travellers to cooperate and act in compliance with the organization's TRM policy and procedures should also be set out. This is sometimes referred to as "duty of loyalty".

The responsibilities outlined in the policy can be developed in more detail in the TRM programme.

5.4 Objectives

The principle objective of the TRM policy should be to ensure that travellers can perform duties optimally, in an environment which is as safe and secure as is reasonably possible, and to have procedures in place to respond to an emergency. The TRM policy should establish the programme and set the boundaries in which this objective is to be delivered.

5.5 Planning/establishing the programme

In developing the TRM programme, the organization should do the following.

a) Ensure there is demonstrable full support from top management with appropriate resources.

b) Ensure a development process that includes engagement with, and input from, internal and, where appropriate, external stakeholders as set out in 4.2.

c) Ensure the TRM function develops a long-term professional understanding with staff in relevant areas to facilitate future, ongoing dialogue.

d) Outline key processes and their interactions.

e) Establish whether the TRM function will be standalone or part of an existing structure.

f) Establish the roles and responsibilities for all duties and roles concerned with the implementation of the programme.

g) Ensure that health, safety and security risks for the programme, including project-orientated operations/assignments, are identified and budgeted for as early as possible. For example, there should be proactive dialogue by the bid and tender teams with the TRM function at offer stage for determining and budgeting the operating risks.

h) Establish the actions needed to ascertain the level of risk for travel. These actions should include, but are not limited to:

   1) determining the organization's overall risk profile in relation to travel risk destinations; this should cover both international and domestic travel (if the home country contains areas considered to be of risk to travellers);

2) listing the categories of risk that can affect the organization, including travellers, for example:

   i) risk to personnel – injury and sickness (including work-related), assault, detention, kidnap, theft, robbery, death;

   ii) legal risk – criminal prosecution or civil legal consequences, or both;

   iii) business continuity risk – failure to overcome an incident and or resume normal operations, system and infrastructure issues;

   iv) risk to reputation – poor incident response or TRM failure can lead to significant reputational damage;

   v) financial risk – failed assignments, trip disruption, taxation, visa/work permit status, civil claims, insurance costs, evacuation costs, medical repatriation;

   vi) risk to data, intellectual property and information assets – breach of data, confidentiality, network, system or loss of assets, espionage;

   vii) risk to productivity/trip effectiveness – trip failure, delays, corporate event failure.

3) Agreeing criteria for decision-making if there are differences of opinion regarding the level of risk and whether the proposed travel itinerary and risk treatment are appropriate.

For further guidance on the pre-planning and development of a TRM programme, see Annex A.

5.6 Implementation

The organization should create an implementation plan. This should be approved by top management and should integrate the TRM function within the organization's operations. It would commonly include the following.

a) Destinations and time frames:

   1) Review and classification of destinations based on an up-to-date risk assessment. Destinations sometimes need to be considered at city/province/region level, as conditions can vary significantly from one place to another, even within the same country. Typically, information would include details on civil unrest, crime problems, terror risk, extreme weather risk, etc. Government and commercial sources are available to assist with this process.

   2) Identification of dates and time frames for events that can have an influence on the health, safety and security of the traveller and can have an impact on the organization's objectives.

   3) Ensuring that travellers are aware of any restrictions or limitations that are imposed by the organization or related service providers relating to insurance, repatriation, use of company resources, specific locations that should be avoided, etc.

b) Traveller-related issues:

   1) The specific risk profile of the traveller. Minors travelling without their legal guardians are a category that requires particular attention. Annex B provides guidance on this matter.

   2) Clarification of how risks arising during off-duty time or personal leave time (both sometimes referred to as "bleisure") are to be managed/covered, if at all, by the organization's travel risk processes.

3) Assessment and provision of relevant training of travelling personnel as appropriate.

c) Processes:

1) Establishment of workable and efficient protocols, including an adequate system for the preparation and recording of all appropriate documents to record, and provide evidence of, work done, and decisions taken.

2) Provision of security awareness, training or other resources for all persons involved in programme delivery, as well as travellers.

3) Procedures for pre-travel authorization, booking of travel and accommodation for the traveller(s). If available, the use of a centralized system for booking travel can provide increased efficiency in managing travel and potential changes of plan.

4) Means, methods and procedures for communications with internal and external stakeholders.

5) Budget ownership and management arrangements.

6) Ensuring the collection and analysis of relevant information (intelligence). This can be done by in-house resources, third-party providers or relevant government guidance.

7) Identification and allocation of responsibilities between in-house staff and external third-party providers.

8) Consideration of the implications for travel during a global disruption. Annex C provides guidance on this matter.

d) Incident management:

1) Ensuring that the organization has an incident and crisis management team, or capability, comprising competent staff with the necessary communication skills, technical tools, instructions and authorization to act when, and how, appropriate.

2) Ensuring, in advance, that appropriate assistance is available, when needed, to resolve safety, security and health issues that can occur. This includes security assistance during travel, notification of relevant events, emergency safety, security and medical assistance, evacuation, and assistance and support after travel.

3) Provision for emergency management and communications. Communications should include both operational requirements, accounting for staff in the aftermath of incidents, as well as managing activities with authorities and public relations.

4) It is important to include the timely provision of information to a nominated emergency contact, or next of kin, if and when appropriate.

6 Travel risk assessment

6.1 General

Risk assessment is the overall process that includes risk identification, risk analysis and risk evaluation. This is based on an understanding of the context of the organization (see Clause 4) and the particular travel arrangements under consideration. All travel should be considered in a risk assessment process.

The elements, methods and techniques of a risk assessment will vary. The overall context, the established principles set out in the organization's TRM policy, and the particular characteristics of the planned travel all contribute to how complex the risk assessment should be.

The scope of the assessment should be defined specifying the dates, locations and modes of travel to which the assessment applies, and any assumptions made. This helps ensure travel is not undertaken outside the scope of a relevant risk assessment

Organizations with a low volume of travel can rely on an ad hoc approach for each travel event. Organizations with high volumes of travel can use relevant technology to automate risk assessments for low-risk locations and trigger individual detailed risk assessments for elevated-risk locations. Such a process can also be used to generate pre-trip advisories that are then provided to the traveller (see 7.4.3).

Risk assessment is primarily used to:

— identify the risk;

— identify the likelihood of an event occurring, and the range of positive or negative consequences if it does;

— understand the significance of the risk to the traveller and the organization;

— prioritize risks that require action;

— enable the organization to make an informed decision about whether to permit the planned travel, in line with the organization's agreed risk criteria and the type of risk treatment that would be appropriate and adequate ahead of and during the trip;

— inform the traveller about the decision made;

— change the nature of the travel and/or the designated travellers.

Travel risk assessments should cover both security threats and safety and health hazards.

Threats are a particular type of risk source. For example, if a specific threat is present then travel to an otherwise low-risk country would need to be considered high-risk travel and measures would need to be put in place.

NOTE Crime and security risk are greater when a motivated offender and suitable target come together in time and place, without appropriate countermeasures present.

Security threats during travel can include:

— crime (ranging from opportunistic petty crime to organized kidnapping for ransom);

— terrorism;

— cyber crime;

— activism (e.g. political, religious, ideological);

— state oppression/repression;

— social engineering;

— aggressive or negative behaviour based on the personal profile of the traveller or the profile of the organization (see 4.3).

Hazards can potentially include:

— health hazards related to infectious diseases and outbreaks, local hygiene conditions or food-borne illness;

— transportation incidents (ground, sea or air travel);

— incidents due to the environment (adverse weather conditions, obstacles, equipment failure, such as sudden technical escalator or elevator events);

— industrial disasters (e.g. explosion, collapse, fire);

— unintentional/negligent activities.

Both security threats and safety and health hazards have the potential for impact on the physical and psychological wellbeing of the traveller and the organization's business objectives.

It is also important to note that travellers themselves can become a hazard because they can be a vector to spread diseases to other workers when coming from or going to places where there can be an endemic or epidemic disease.

It is recommended that travel risk assessments are completed in an inclusive and collaborative way involving the traveller and relevant internal stakeholders. For elevated-risk travel, including travel to high-risk destinations, high-profile visits or travel involving high-risk activities, organizations can use external specialist providers.

The results of risk assessment should be recorded to inform decisions regarding risk treatment options. Where organizations use technology to authorize low-risk trips, this may be achieved by the traveller's acknowledgement of receiving and reading their pre-trip advisory.

Further information on risk assessment can be found in ISO 31000:2018, 6.4, and IEC 31010.

6.2 Risk identification

The purpose of risk identification is to find, recognize and describe risks that can impact an organization's ability to achieve its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

There are various sources of information available for the identification of travel-related risk. These include open source and proprietary information.

Internationally and locally sourced information, such as open source government statistics, can provide objective data relating to crime statistics, geopolitics and risk ratings for the location(s) being assessed. An organization can have travellers with relevant previous experience who can be consulted.

National government foreign affairs ministries and embassies can be useful sources of information and advice. In addition, local government agencies can provide more location-specific crucial information on health, safety and security matters, including legislation, that are relevant to a particular trip.

Organizations can decide to contract external travel security experts to perform parts of the risk identification for the organization.

Risks can be associated with objectives for the safety, security and health of the traveller, or with other organizational objectives. If there is a potential conflict between these objectives, the organization should give priority to the traveller. Categories of risk such as those in 5.5 list item h) 2) can be useful. However, they should not limit thinking, not least because there can be other factors specific to the context of the travel that need to be considered. Tools such as those described in IEC 31010 can be used to help identify risks.

The organization should consider emerging or evolving risks that can contribute to traveller and operating risk. These have high levels of uncertainty with one or more further characteristics (e.g. volatile, complex, ambiguous, chaotic, interconnected, interdependent, medium-/long-term, uncontrollable, wide-reaching). Examples of emerging or evolving risks include cyber risk, increased frequency or intensity of adverse weather, and regional or pandemic infectious disease.

6.3 Risk analysis

The purpose of risk analysis is to comprehend the nature of the risks identified (see 6.2) and their characteristics. Analysis techniques can be qualitative, quantitative or a combination of the two depending on the circumstances and the decisions which need to be made. Risk analysis involves a consideration of uncertainties, sources, causes and drivers of risk, consequences, likelihood, events, scenarios, controls and their effectiveness.

Sources of intelligence that inform risk analysis include historical information, expert advice and statistics.

Risk analysis should consider factors such as:

— the likelihood of events and consequences;

— the nature and magnitude of consequences;

— complexity and connectivity;

— time-related factors and volatility;

— the effectiveness of existing controls;

— sensitivity and confidence ranges.

The TRM policy should include an escalation process if the level of risk identified is significant, especially if there is threat to life.

6.4 Risk evaluation

The purpose of risk evaluation is to support decisions. It involves comparing the results of the risk analysis (see 6.3) with the established organizational risk criteria to determine the value of taking additional action.

Decisions can involve evaluating whether travel should proceed, be cancelled or be replaced by alternative means of engagement or communication. Alternatively, they can involve revising objectives.

Assuming travel is to take place, further evaluation needs to establish:

— whether existing generic controls are appropriate to the particular circumstances and identified risks;

— whether new controls can better treat the risk, for example:

  — alter the itinerary to limit risk exposure;

  — adjust the number/profile of people travelling to limit risk exposure;

  — adjust the mode of transport (e.g. flying rather than overland);

  — reduce the number of days of travel;

— which of several options for travel arrangements should be selected on the basis of risks, costs and benefits;

— whether the residual risk is acceptable or the decision to proceed with travel should be revisited.

Decisions should take account of:

— the context and purpose of the travel;

— the wider context and the actual and perceived consequences to external and internal stakeholders;

— the costs and benefits involved;

— the traveller profile;

— the nature and magnitude of the risks involved.

Where circumstances are commonly encountered, it is sometimes possible to make a decision based on experience and organizational TRM policy and rules or to use fairly simple expressions of risk criteria.

Where the situation is novel or there is high uncertainty (as is often the case with high-consequence risks) risk evaluation often involves a more deliberative and consultative process taking account of detailed information from risk analysis.

It can be necessary to seek further information and undertake further analysis in order to make a good decision.

7 Travel risk treatment

7.1 General

Based on the risk assessment, the organization should ensure that controls address risks prior to travel, during travel, during and after incidents, and once travel is completed. Such measures should be tailored to the destination and the individuals travelling, their activities and the information they bring with them.

One or several treatment options can be required to modify risk to an acceptable level. The same treatment option can also affect multiple travel-related risks. Treatment options should therefore be selected in consideration of the range of risks affecting the specific proposed travel, rather than considering each risk in isolation. A range of treatment options, relevant to travel risk, are set out in this clause.

Top management is accountable for ensuring that arrangements are in place for managing risk associated with travel. Multiple individuals, including management, contracted providers and travellers themselves, are responsible for managing these risks. This includes responsibility for ensuring that treatments are implemented that modify risk to an acceptable level.

Decisions about the selection of treatment options involve judgements balancing the overall advantages (tangible and intangible) and disadvantages (disproportionate costs and other adverse effects) that can occur, and how these can affect the objectives for the proposed travel as well as the overall organizational objectives. However, selection is broader than a solely economic matter when it affects risks to travellers.

A risk can have more than one risk treatment option, and a risk treatment option can apply to more than one risk.

Treatments need to be monitored and reviewed continually in order to ensure that:

— any change in context or the nature of risk is reflected in considering the need to further modify risk treatments;

— risk treatment strategies continue to meet the agreed objectives for those treatments;

— organizational capacity is sufficient to continue implementing risk treatments and deliver on objectives;

— risk treatments are not adversely affecting other controls or changing the nature of other risks.

7.2 Risk avoidance

7.2.1 Pre-travel authorizations

A pre-travel authorization and booking procedure should be established to ensure all planned travel is recorded, visible to the TRM function, assessed and approved in line with the agreed TRM policy, programme and risk criteria. Such a procedure can also be used to reduce risk.

The procedure should assist planning for the relevant trip by identifying any relevant medical (e.g. vaccination) or visa requirements. It should also provide the TRM function with the data required to react quickly in the event of an incident.

The procedure is a means for approval to be informed by the overall risk to the organization rather than just the travellers' objectives. This can be achieved by ensuring approval is by senior management or outside the normal line management. The level of seniority with approval authority should reflect the risk associated with the trip.

A mandatory booking process should be developed to clearly outline the booking channels that can be used for all forms of travel, transport and accommodation.

NOTE As appropriate to the nature and volume of travel, organizations can choose to use a technological platform for the booking process. This can also be used to triage trips, e.g. triggering automated authorization for low-risk travel while flagging other travel for closer scrutiny.

7.2.2 Restrictions

Restrictions can be used to treat various travel risks. For example:

— high-risk travel can be avoided by using remote meeting technology;

— specific security-related risks can be avoided by, for example, limiting:

  — the type of transports used in certain locations and situations;

  — the time of day that movement is permitted;

  — movements in a specific location at the destination;

— risks relating to data protection and privacy can be reduced by limiting the information, devices and assets taken on travel;

— the loss or delay of key personnel, and the potential impact on business continuity, can be avoided by limiting the numbers of travellers being transported together in the same vehicle (e.g. airplane, boat, car);

— risks to travellers in high-risk locations can be reduced by restricting the length of time spent in the location as well as factoring in the traveller's personal profile;

— the risk to trip effectiveness and safety and security can be reduced by considering public holidays and environmental factors at the location.

Restrictions can also apply to the types of accommodation. See Annex E.

NOTE Avoiding one risk can involve introducing a new risk and can also restrict opportunities.

7.3 Risk sharing

7.3.1 General

In the context of TRM, risk sharing can involve a distribution of risk and allocation of the associated liabilities in the clauses of a contract. If a contract with a third party is used, the agreement should clearly outline how any allocation is done, i.e. through contractual transfer, indemnification or commercial insurance.

Risk sharing should be considered as complementary to, and not an alternative to, TRM.

7.3.2 General insurance

The organization should ensure adequate and appropriate insurance cover is in place in line with risk assessments, taking into account varying national and international requirements.

Insurance, including liability insurance, should be provided to cover a range of potential issues such as:

— cancelled/delayed flights and lost luggage;

— injury, medical emergencies and death;

— terrorism, cyber crime, theft and criminal damage;

— evacuation and repatriation.

The organization should be aware of any special exclusions in the policy coverage.

This organization should also verify whether any service providers are adequately and appropriately insured. The organization's insurance providers should be made aware of any third-party service providers that do not have reasonable insurance coverage.

7.3.3 Specialist insurance

Special risks insurance can be used to provide cover against conflict risks, kidnap and ransom, and loss of key personnel.

Kidnap and ransom insurance is an important consideration for an organization sending travellers into locations with known kidnapping and ransom threats. This insurance cover typically also provides access to specialist consultants to help plan for and manage an incident.

Use of this kind of insurance is usually a highly sensitive and confidential matter, with knowledge of the coverage restricted to very few people in the organization. The TRM function and appropriate members of the crisis management team should be involved in the procurement process of such coverage so that escalation procedures can be devised and included in incident management planning.

In countries where it is legal, specific "key person insurance" can provide cover against the loss of key or commercially important people to the organization.

NOTE In some countries, legislation prohibits kidnap and ransom insurance. In those cases, this subclause would not be applicable.

7.4 Risk reduction

7.4.1 Selecting treatment options

Risk treatment options are most commonly identified and selected to address the sources of risk. These sources can include, for example:

a) travel destination or circumstances/risks at the travel destination;

b) accommodation;

c) travel route;

d) travel itinerary;

e) travel duration;

f) traveller and organizational profile;

g) relevant geopolitical circumstances;

h) relevant government/regulatory advice;

i) cyber threats;

j) significant cultural and religious differences;

k) access to critical infrastructure and resources;

l) contextual risk factors such as extreme weather, natural disaster, conflict, epidemic/pandemic, reliability of communications, etc.

7.4.2 Competence

The organization should do the following.

a) Set minimum competence requirements for travellers and for those responsible for managing travel or response to incidents impacting the organization's travel safety, health and security performance and compliance requirements.

b) Periodically review the competence of travellers and those involved in TRM. Components of the assessment should be defined. This can include a review of documents such as incident records, risk assessments, good practices and suggestions from other organizations (such as assistance providers, insurance providers, governments and other institutions).

c) Consider appropriate education, training and experience in the competence assessment.

d) Identify training needs associated with travel safety, security and health. See Annex F for further guidance on training.

e) Take actions to support gaining necessary competence (if appropriate) and evaluate the effectiveness of the actions taken (e.g. training, mentoring, re-assigning travellers, hiring or contracting competent providers).

f) Ensure the selection of providers and sub-providers includes verifying competence and experience that demonstrates:

   1) appropriate accreditation, certification and licences;

   2) evidence supporting prior relevant experience and their reputation, both professional and ethical (if appropriate, this should also include a vetting process);

   3) geographical reach that will support potential travellers at the desired location.

The organization should retain appropriate records as evidence of competence.

7.4.3 Information, advice and updates

An organization should do the following.

— Proactively source relevant and reliable information and advice to provide to its travellers prior to and during travel. This should be location-specific and highlight the medical and security levels of risk. The findings of risk assessment can be a source for such information and advice.

— Ensure that services and a process are in place to ensure that travellers are provided with timely updates that can affect their safety and security during travel.

— Implement a process to ensure that travellers have received and acknowledged the information and advice provided.

7.4.4 Communication protocols/platforms

Communication protocols are critical in responding to any incident. Key stakeholders should be well trained and practised in their responsibilities. They should have the knowledge and ability to use the designated platforms to trigger an incident management response. This should include appropriate procedures to be used when under duress (e.g. the use of a recognizable code or expression to indicate an individual is in trouble) within its communications protocols.

In planning, the organization should consider the methods that are available for mass communication, such as specialist tools or service providers, the intranet and social media platforms to quickly disseminate information.

An organization should take into consideration that the use of some specific technological equipment in certain countries is subject to legal restrictions.

7.4.5 Accommodation selection

An organization's TRM policy and selection process for accommodation, including hotels, serviced apartments, short-term rental or "shared economy", should be risk-based. Individual on-site assessments will not be necessary in all cases.

For low-risk locations, the assessment can be carried out using evidenced-based questionnaires to confirm the standards of health, safety and security the accommodation providers have in place. The TRM function should be involved in defining the questionnaire and analysing the results.

Where an individual or on-site assessment is considered to be appropriate, an organization should use competent internal or external assessors.

For accommodation in higher-risk locations, additional specific safety and security capabilities should be assessed, as well as any previous incidents (see Annex F).

Some organizations refer to "preferred" or "approved" accommodation in their travel programmes. Traditionally, these are primarily focused on considerations such as room types and rates, cancellation policies and the range of services available, etc. and do not always address the health, safety and security risks addressed in this document. Organizations should therefore ensure that, if such terms are used, they are inclusive of health, safety and security considerations.

There are also third-party assurance schemes that carry out structured, evidence-based evaluations of the standards of health, safety and security arrangements in place in hotels. These can be referred to as "certification" and "accreditation".

When an organization chooses to use such an assurance scheme, it should exercise due diligence to assure itself about its scope, design and operation. Matters to consider can include:

— the scope of the scheme;

— how the scheme gathers the evidence on which it bases its assessment, e.g. based on questionnaires or on-site verification;

— whether it is based on assessments of individual hotels or of corporate policies that apply to a chain of hotels;

— the frequency of detailed assessments;

— how the scheme takes account of changing or emerging risks;

— whether the scheme itself is independently validated in some way.

7.4.6 Information security and privacy protection

An organization should carefully consider the data protection, information security and privacy requirements relative to its business, the assignment and the traveller, and implement appropriate measures to manage these risks. The organization should ensure it has considered consent, and has access to competent advice on information security and privacy protection. This can be available within the organization or with the assistance of external specialists, or both.

Organizations should ensure that information is properly protected and secured to avoid consequences which can impact the travellers' health, safety, security or privacy, or the organization's objectives. Organizations should identify relevant data privacy legislations [e.g. the Health Insurance Portability

and Accountability Act (HIPPA) in the US and the General Data Protection Regulation (GDPR) in Europe] and plan and proceed accordingly.

Sources of information include:

— information generated, collected, stored or processed by the organization or third parties, such as traveller, itinerary and location data;

— information that the traveller takes or uses during travel, or returns with.

Key considerations on information security and privacy protection should include:

a) intellectual property;

b) medical data, and personal profile data, which can require additional controls since it is highly sensitive personal data and can be subject to specific regulation in different jurisdictions;

c) ensuring that any proof of life documentation is stored in a highly secure manner and has emergency access protocols in place;

d) data transfers between the organization and third parties;

e) security of the information systems or media used to store the information;

f) ensuring that all data generated, collected, stored or processed by the organization or third parties through the platforms, tools and applications are secured;

g) ensuring that all travellers' privacy concerns are addressed;

h) ensuring that all systems and processes are regularly reviewed and audited;

i) ensuring secure communications methods are available during travel to avoid the use of unsecured networks, particularly when communicating sensitive information;

j) the potential implications of using personal devices for work purposes;

k) remote access to work-related information or data while travelling overseas on personal leave;

l) the use of information technology (IT) in the destination and any restrictions that can apply;

m) ensuring travellers are aware of situations which can compromise information, such as being required to unlock their mobile devices or enter their laptop passwords, including social media accounts, when entering certain countries, which can also happen to business travellers who are subject to unannounced inspection by authorities (e.g. dawn raids);

n) ensuring travellers are aware of social engineering, compromising situations, baiting, etc.

For further information on information security, cyber security and privacy protection, refer to the ISO/IEC 27000 family of standards.

7.4.7 Transportation

An organization should assess all the appropriate modes of transportation to be used by travellers including air, maritime, trains, buses, taxis and shared economy transportation.

Organizations should have a policy on which airlines to use. In addition to routes, pricing, quality of service, timeliness, etc., the policy can consider factors such as safety record, hygiene measures, financial wellbeing/credit worthiness, etc. It can refer to external open source sites such as the International Air Transport Association (IATA) or national air transport regulators.

For low-risk locations, the organization should outline the need to only use pre-arranged transport or official and authorized public taxis.

In high-risk locations, ground transportation should be carefully planned and appropriate service providers should be used. The risk assessment should determine whether secure transportation is required.

The organization should assess using the services of ride-share companies as both a general and specific local policy. This should take into account potential security risks faced by travellers, notably in high-crime locations and where the use of ride-sharing services is either contested or effectively regulated.

7.4.8 Journey management

There are some situations for which an organization should establish enhanced journey management arrangements prior to travel. These can include, for example, travel to high- or extremely high-risk destinations or the profile of the traveller in a particular location. These measures can include a more detailed travel route assessment, meet and greet service, additional security assistance, safe accommodation selection, etc. reflecting the traveller's profile and the ground level of risk.

An organization should make plans to manage any unexpected changes to itineraries. An analysis should be completed to determine possible flaws in the journey management.

Journey management can be achieved via internal resources or a third-party provider.

7.4.9 Medical and health risk reduction

7.4.9.1 General

Organizations should consider appropriate checks for all travellers to ensure they are medically fit (both physically and mentally), for the travel planned and can cope with the additional stress that travel can bring. Such checks should consider pre-existing or multiple coexisting health conditions.

Post travel checks can also be appropriate, particularly if the traveller is or has been involved in stressful situations or events.

Travel, working in unfamiliar locations and pressures to complete multiple tasks in a limited time can be stressful. The organization should take steps to reduce stress (e.g. planning of business meetings to ensure time for adaptation to a new routine or time zones) and provide appropriate advice for travellers so they are aware of their physical and mental limits.

Organizations should assess the ability of the destination country to support travellers with emergencies and pre-existing conditions.

When travellers are coming from, or going to, a place where they can become a risk to other workers because of endemic or epidemic diseases, appropriate treatment options should be considered before and after travel. Examples of measures can include testing and quarantine before or after travelling, preventive treatment for both the traveller and co-workers. Health certificates, test results and vaccination cards can be confidentially available in paper or digital format as required and appropriate for the traveller.

Organizations should consider the use of occupational health and safety expertise to assess programme requirements as well as to support medical risk assessment and treatment.

7.4.9.2 Traveller recuperation

The organization should do the following.

— Consider the impact that frequent business travel can have on the health of business travellers. It should consider consulting or employing occupational health practitioners to assess travel-related stress, injury, illness and the need for recuperation. This assessment should also include examining the effects of long-haul flights or road/rail travel.

— Provide clarity on what rest and recuperation travellers are entitled to following travel.

The amount of rest and recuperation should be tailored to circumstances of the trip, and should consider:

— the length of the flight, including layovers and connections;

— time differences;

— the class of air travel (including the ability to rest/sleep);

— the intensity of activities undertaken during travel;

— the destination (e.g. high-risk or not);

— any physical or psychological medical conditions;

— incident(s) that can have occurred during travel.

7.4.9.3 Medical treatments

An organization should ensure that travellers have access to professional medical advice in order to determine if medication or vaccinations are recommended for their trip, or if any medications are considered illegal in a layover or destination location.

Travellers should ensure they have sufficient medication for the duration of the planned travel, plus reserve quantities in case of travel disruption. This should include both medication they take regularly and also medication they need to take in response to irregular and unpredictable health episodes.

Medication licensing arrangements can vary significantly between countries, both in terms of access to medication over the counter and prescription-only medication. Trade names of the same drug can also vary across countries. Given both these issues, consideration should be given to:

— travellers taking appropriate medical certification and information regarding principal components and dosage for any medication they take with them;

— travellers taking a medical certificate (or other acceptable evidence) with them to justify possession and use if they take medication with them that is not approved in the places to be visited;

— obtaining assurance in advance that the medication is available (and under what name) in the country to be visited, if the intention is to rely on sourcing it there.

The organization should facilitate the provision of vaccinations and medicines related to the travel, and any pre-trip testing requirements in line with specialist advice.

The organization should ensure that any medical information deemed to be sensitive by the traveller is respected and treated as strictly confidential. See 7.4.6.

Many risk factors can be exacerbated by the remoteness of a destination and the ability to medically evacuate a traveller. To mitigate these risks, it is good practice, where appropriate, to provide the traveller with a medical kit.

7.4.9.4 Travellers with special needs

For some travellers it can be appropriate to prepare a specific medical response plan should they experience health problems while abroad.

The organization should consider whether particular requirements are necessary for travellers with special needs. For example, it should ensure that airlines and hotels are able to provide the required assistance, paying particular attention to wheelchairs, service animals, etc.

7.4.10 Medical and security support services

The organization should, after a risk evaluation, consider its needs and capacity regarding continuous medical and security support services. Third-party service providers and sub-providers can be used to assist, where required, with medical and security advice and support prior to, during and post-travel. Such support can include the assessment, provision and dissemination of information, advice and updates and, where appropriate, this should include practical and logistical support.

Many medical emergency providers have tools/apps whereby the travel destinations, doctors, hospitals and other medical providers can be found and located. Such tools can help enable the traveller to self-help.

The organization should make arrangements to ensure that any necessary medical and security assistance can be secured and funded.

Security assistance can include:

— on-site briefing;

— security driver(s) (with or without the backup of armed or unarmed security personnel);

— overt or covert close protection;

— liaison with public security agencies.

The organization should ensure appropriate coordination with such providers both locally and with the organization itself.

Such providers and sub-providers should be carefully selected to ensure both their competence and experience. Subclause 7.4.2 list item f) provides guidance on matters to be considered.

Subject matter experts and the TRM function should critically review the advice being disseminated and the services offered by third-party service providers to confirm they are adequate and objective.

The organization should be aware that it is accountable for decisions made by third-party providers acting on its behalf.

Further information on the contracting of security service providers can be found in ISO 18788:2015 and References [9] and [10].

7.4.11 Incident management planning

Incident management measures should be based on risk assessment and should be appropriate, proportionate and dependent on location.

The organization should provide clear incident and near-miss reporting procedures and templates to all travelling staff.

The organization should address global as well as local incident response planning and implement appropriate measures. These measures should address:

— preparedness;

— treatment;

— response;

— recovery;

— adaptability;

— incident reviews.

The organization should have a written incident response plan which describes the authorities and responsibilities of key personnel including the incident management team. This team should be constituted and resourced to manage situations that need coordination internationally or locally, or both. This plan should be appropriately communicated.

The incident management team should be multidisciplinary, led by top management and supported by a designated incident management coordinator and a communications professional (or their designates). In smaller organizations, these responsibilities can be shared.

Ideally, the members of the incident management team should include people selected from the list of internal stakeholders set out in 4.2 with prior experience of dealing with relevant areas.

Organizations should assess their capacity to respond to a critical incident and activate their incident response and evacuation/repatriation plans. The assessment should include:

— training;

— regular exercises to simulate incidents and rehearse response scenarios in a coordinated and timely manner;

— access to information;

— financing and local resources;

— adequate medical and security support on location (see also 7.4.10), which should include, but is not limited to:

  — an organization's dedicated resources (local or deployable);

  — medical, security and emergency services;

  — external providers;

  — appropriate government agencies.

An organization should define communication protocols as part of incident management planning. Such protocols should cover communications between stakeholders as well as technological measures.

Reports derived from the investigation of incidents requiring intervention or assistance, as well as near-misses, should be used as a source of information for the prevention, or reduction in severity, of future occurrences.

NOTE Further information on business continuity can be found in ISO 22301.

7.4.12 Incident and emergency contact points

An organization should develop procedures to enable travellers to communicate urgently should they have any safety, security or health matters.

Typically, this would involve a designated emergency contact point available at any time from where they are located and should include specific escalation protocols.

These procedures can ensure that travellers are referred to those best positioned to provide immediate support. This will vary depending on the nature and severity of the incident or emergency, but can include:

— medical assistance providers/insurers;

— local police;

— host;

— security provider.

It is important that processes are in place with any contracted external providers to confirm that the organization would be notified if and when any of their travellers contact them for urgent assistance.

Organizations should consider the use of local emergency services, where appropriate, as a contact point. The contact point can be provided in-house or by an external provider. If the contact point is external to the organization, it is important to have procedures to liaise with in-house stakeholders.

The traveller should be provided with adequate and appropriate instructions for implementing the procedures. This should include a convenient and accessible means to reference their emergency contact protocols, such as a plastic card.

The systems selected for communication should be readily available to the traveller. Their use should be operational at the location concerned.

There should be a backup procedure, established in advance, on a case-by-case basis, if communication with the emergency contact point is not possible.

During emergency situations, communications systems, networks or personal equipment can be compromised. It is, therefore, important to consider alternative means of communication (phone, SMS, email, notifications).

7.4.13 Traveller tracking

Traveller tracking arrangements, or manual reporting-based tracking, are of great importance in TRM.

Knowing the location of personnel is essential to warn them of threats and hazards, and to protect them during and after an incident. The nature of these arrangements will vary between organizations depending on the volume of travel. Large organizations with high volumes can use an IT-based system, whereas for smaller organizations with low volumes manual systems can suffice.

There are three methods whereby travellers can be tracked.

a) Itinerary-based: These systems collate booking information relating to all kinds of transportation and accommodation. They are only an indicator of where the traveller is supposed to be, but can be supplemented by the traveller checking-in at agreed points and frequency.

   These systems can also help to implement a pre-travel authorization procedure and assist in disaster recovery situations where local conventional communications systems are unavailable.

b) Expenses-based: These systems monitor expenditure and sometimes also itineraries. They are, however, only an indicator of where the traveller has been.

c) Technology-based: These systems use technology to track, monitor and record movements and precise location. They provide the most accurate data as to where the traveller actually is. However, they are subject to availability, user capability, and power and connectivity requirements, which can be compromised during or after an incident in certain locations. It should be noted that all such technology tracks only the electronic devices onto which it is loaded and not the person carrying it.

An organization should assess the need to actively track travellers. Privacy and information security concerns, costs, consent, data protection and any other relevant legislation should be carefully considered before implementing a technological solution.

It may be considered more acceptable to only track travellers in this way in high-risk locations, or under particular circumstances for very high-risk profile personnel.

The organization should have a process in place to follow up and intervene in circumstances where the traveller is unable to report in following an incident, e.g. because they have suffered a serious injury.

7.4.14 Kidnap and ransom planning

Where appropriate, the organization should ensure that kidnap and ransom is incorporated in incident management planning.

This should predefine the organization's status with respect to access to funding and, in countries where it is legal, specialist insurance in the event of such an incident occurring.

The provision of kidnap and ransom insurance is not only reimbursive as an insurance policy but can also be a countermeasure. This is because it typically provides access to professional and experienced crisis management teams to assist with planning for, verifying and dealing with a confirmed incident.

Kidnap and ransom insurance coverage sometimes also provides access to specialized training for the TRM function and other key stakeholders.

Knowledge of kidnap and ransom insurance cover can act as an incentive. It is imperative that an organization ensures that there are robust controls relating to the traveller's knowledge relating to the insurance policy and coverage.

An organization should assess and consider the need for appropriate means to confirm the identity of a traveller in cases of kidnapping, abduction or detention. This can include "proof of life" documentation or other personal or physical identifiers to aid the verification of an incident, and the liaison with emergency contacts. This can require support from relevant experts, such as those provided by specialist insurance providers.

7.4.15 Evacuation planning

An organization should, with relevant third-party providers, as appropriate, plan for the potential need for relocation, shelter in place or evacuation of personnel from affected areas. This can arise for a number of reasons, e.g. a medical or security-related incident, injury, political instability, or a natural or environmental incident. Such considerations should be incorporated as part of the pre-travel risk assessment and integrated with any country-level evacuation plan. They should take into account the profile and nationality of the traveller, including their passport information, which can impact on likely viable international safe havens. Such relocation or evacuation can be to a safe or appropriate location within the country or to another country. Planning for evacuation should consider any relevant protocols in the destination country.

Evacuation planning for health-related incidents can be required as some high- and medium-risk medical locations or facilities can be inadequate and so any hospitalization requirements need to be fulfilled by transporting the traveller out of country.

Medical repatriation can be provided by third-party providers (e.g. as part of a medical membership package or an insurance policy). Such repatriation can be to the nearest country with suitable medical services rather than to the home country.

Evacuation planning for security-related incidents can be more challenging for an organization as it is possible that normal modes of transport will not be available, e.g. airport or seaport access for external aircraft or vessels can be restricted. This can result in the need for secure ground transportation to a neighbouring city or country. In some cases, movement will not be possible, and some locations require provision for a period of no movement (sometimes referred to as "stand-fast").

8 Communication and consultation

8.1 Programme/strategic communications

An organization should ensure that the development of the TRM policy and procedures for its implementation engage relevant internal and external stakeholders as set out in 4.2.

The agreed TRM policy and procedures should be effectively communicated throughout the organization so that potential travellers, and their managers, understand them and travellers are aware of travel risks and how the organization controls and manages them.

There should be communication between the individual/groups responsible for the TRM function and a TRM process (e.g. assignment). In micro- or small organizations, these can be the same individual/group.

Adequate information for planning and implementing, and, where relevant, changing, assuring or terminating a TRM process (e.g. assignment), should be available and communicated.

Issues to consider include the following.

a) The TRM policy and programme should be communicated to, and acknowledged by, travellers.

b) Travellers and other relevant stakeholders should be engaged in the risk assessment process and in the identification and selection of risk treatments.

c) Travellers need to be aware of:

   1) the actual or potential impact of travel risks on their work productivity, safety, security and health;

   2) the risks the traveller can be exposed to during travel and how to identify them;

   3) how they can contribute to effective management of travel safety, health and security.

d) Travellers need to understand:

   1) the benefits of following the TRM policy and procedures;

   2) the implications of not doing so, with respect to managing risks and failing to meet legal and other requirements;

   3) their requirements to be engaged in the employer's duty of care through following the policies and procedures in place to protect them, and their organization, from foreseeable harm (this is sometimes referred to as the "duty of loyalty").

e) Multi-channel communication should be considered. Mass emails or social media can also be appropriate, recognizing that communication tools evolve rapidly and communication techniques should be responsive to this.

f) From a "business as usual" perspective, formats such as emails, team meetings and noticeboards can be used to convey information and updates.

g) Means to facilitate personal communications (which can be two-way) should be provided.

If third-party providers are used by the organization, the content and timing of communications with them should be considered.

8.2 Operational/technical communications

Depending on the size and complexity of the organization, and the circumstances of the travellers (e.g. in a remote rural area without smartphone coverage), detailed and robust operational communications frameworks should be in place to deliver the TRM policy and procedures.

Issues to consider include the following.

a) For specific travel, it is recommended that if customized briefings/training/advice is needed, an auditable record should be generated and kept.

b) Aide-memoires describing the process and procedures which can be activated in an emergency should be provided to travellers.

c) In TRM it is often the case that a timely update can be very important (e.g. if travellers are in an area impacted by a natural disaster). In this case, all stakeholders should be informed of issues related to travel safety, security and health as soon as the details are confirmed.

d) In case of an emergency it is vital that communications reach the appropriate stakeholders without delay. SMSs or text messages can be more reliable than internet-based communications in some locations. There are platforms available where mass SMSs or text messages can be sent (similar in concept to a mass email), although these need to be kept under regular review as such platforms can also be withdrawn.

e) In remote rural areas, solutions can range from radios to satellite telephones (but note the unauthorized use of such phones is illegal in some countries).

f) How to activate the TRM team and escalate internally to the corporate level (incident management team, crisis management team or similar) as required.

g) If an organization is using the services of a specialist TRM service provider, there should be a clear escalation protocol for engaging such services, if needed.

h) If an organization does not have an arrangement (retainer or similar) with a specialist TRM service provider, ad hoc assistance can be required in some circumstances. In anticipation of this, an organization can engage with TRM specialists in advance and the contact details can be made available.

9 Programme monitoring and review

9.1 General

The organization should evaluate the effectiveness of its TRM programme involving all relevant internal stakeholders to identify strengths and weaknesses to guide further development and improvement. The organization should put into place evaluation, monitoring and review processes to see how efficiently and effectively it is at carrying out travel safety, health and security policies and arrangements. This should take place at all stages of the TRM process by people with the necessary competence. If service providers are engaged, organizations should consider how they can help with programme monitoring and review.

The extent, frequency and trigger (periodic, event-based or other change in circumstances) for monitoring and review will depend on requirements and context. At a minimum, a full review should be conducted annually, with a focus on improvement and incorporating lessons learned. In addition to a scheduled annual review, there are various circumstances that should trigger a review to allow for the new situation. Such circumstances can include, but are not limited to, changes in:

a) the assignments requiring travel;

b) locations where the organization will be sending staff;

c) the level of risk in a location where the organization already has significant operations (e.g. there has been a significant political change in a certain nation);

d) the organizational profile or the demographics of travelling staff (e.g. new staff with certain nationalities/citizenships/ethnicities/religions can have ad hoc considerations in some locations);

e) legal or regulatory requirements;

f) global best practice for TRM, a change in TRM staff within the organization or a TRM policy change within the organization;

g) knowledge and experience following a significant incident or near miss in the organization or industry, or both;

h) products or services;

i) policy or practice with respect to outsourcing elements of TRM.

As reviews are completed and the TRM programme is updated, it is crucial to ensure that all stakeholders are informed. This can include service providers, sub-providers, internal staff and, of course, travellers. Where relevant, TRM documentation should be updated with appropriate details including date, version number, updater and approver.

9.2 Surveys

Surveys should be designed and used to identify gaps, improve programme effectiveness and highlight changes in conduct, compliance and security culture. The surveys should cover important aspects of the TRM programme such as the initial briefing, training, support while travelling, and the post-travel debriefing.

To ensure the most accurate metrics, it is recommended that all relevant staff are surveyed. Surveys submitted on a voluntary basis tend to only include highly negative comments (and occasionally highly positive); however, the majority of travellers will go un-surveyed. The actual survey should be user-friendly, non–intrusive, ideally IT-based for ease of data compilation and a compulsory part of completion of any travel (e.g. a short survey attached to the end of the travel reimbursement process or similar).

Debriefs, observations and interviews can also be used to determine if there is a change in risk attitude or culture.

9.3 Benchmarking

An organization should regularly engage in benchmarking exercises with organizations of similar size, industry and geographical exposure to share knowledge and compare third-party service provider performance. This can be done through a formal process, but also less formally through participation in seminars, etc. to share knowledge and best practice.

Benchmarking can also be internal where there is a process in which an organization will determine best practice for TRM and use it for comparison and continuous improvement.

9.4 Metrics

The TRM function should identify, collate and track programme key performance indicators to provide stakeholders with actionable metrics to evaluate and increase programme effectiveness. Key indicators can include:

a) the number and details of the organization's individual travellers;

b) the organizational footprint, both expatriate and travellers;

c) travel by category (e.g. risk rating, date, location);

d) completion of pre-travel health medical assessments;

e) the number (and percentage of total) of cases where:

   1) a required pre-travel briefing was not carried out;

   2) pre-travel advice prompted an amendment to the travel plans (and associated costs, if any);

   3) travel was not approved because of a high level of risk;

   4) training was provided specific to the travel;

5) assistance during travel was required (and associated costs, if any) or contact was made to medical or security emergency providers, or both;

6) a required post-travel briefing was not carried out;

7) an increase in cost could have been avoided;

f) third-party service provider performance – logistics, security, medical emergency, etc.;

g) mandatory procedure compliance/noncompliance by type.

10 Programme recording and reporting

10.1 General

Record-keeping and reporting of risk management results assist in:

— satisfying legal and regulatory requirements;

— decision-making;

— improving programme activities;

— improving cross-functional interaction;

— enabling the auditing of the TRM system/programmes.

Records should be maintained in accordance with the organization's record management practice.

10.2 Documentation

Documentation should include:

a) copies of passports, visas and essential documents;

b) traveller profile information including vaccination record, emergency contacts, next of kin and relevant pre-existing medical conditions;

c) a traveller aide-memoire of crucial contact details, in case their standard contacts database (e.g. smartphone) is not accessible;

d) escalation procedures:

1) at the corporate/strategic level;

2) for the local office (where an incident can occur);

3) aide-memoires for the traveller;

e) incident management plans:

1) at the corporate/strategic level;

2) for the local office (where an incident can occur);

3) aide-memoires for the traveller;

f) evacuation plans:

1) at the corporate/strategic level;

2) for the local office (where an incident can occur);

3) aide-memoires for the traveller;

g) proof of life documentation (as discussed in 7.4.14);

h) a mechanism to ensure documentation is reviewed and updated regularly (ideally annually);

i) procedures for documentation access in emergencies;

j) confidential data and privacy concerns – the latest policy direction from a corporate/strategic level;

k) insurance contacts to turn to for support;

l) an insurance summary describing insured areas.

10.3 Recording and reporting

It is crucial that all relevant data are appropriately recorded and reported as part of an organization's duty of care and compliance. From a good practice and business continuity perspective, TRM typically results in a large number of processes/procedures and also data/metrics, which should all be stored appropriately.

A primary source of data is the TRM programme documentation (see 10.2) and metrics (see 9.4).

Irrespective of the size or complexity of the organization, some primary considerations for recording and reporting of data should be:

a) a detailed repository of information for all travel, in particular high-risk travel;

b) travellers reporting of their own experience on the risk and threat after travelling, as necessary;

c) detailed recording of any incidents to provide a basis for learning lessons and evidence of the organization's response;

d) detailed recording of risk assessments and controls used, including:

1) the name of the risk (short name);

2) a description of the risk that clearly and unambiguously explains the risk;

3) the data used and assumptions made (e.g. additional information about the risk, its source and other potential causes such as industry, the organizational profile, traveller profile, location of operation and type of operation);

4) who was involved in the risk assessment process;

5) the conclusions of the risk assessment;

6) agreed risk treatment options;

e) records of informed consent (permission granted in full knowledge of the possible consequences) – the process by which travellers are informed of the safety and security risks to which they can be exposed during the course of their activities and they are provided with the ability to either accept or decline these risks.

There are many options for collecting and recording these data. A recommended methodology is to categorize each assignment/journey as a "trip" (or similar), with the data being recorded based on the details of that "trip".

Depending on the volume of travel, recording the data using an IT system can provide an efficient mechanism for generating reports to:

— identify strengths and weaknesses with TRM;

— assign resources;

— adjust procedures based on trend analysis;

— provide advice to the project at a senior level.

The detail and sophistication of reporting is informed by the nature and volume of organizational travel. It can range from being internally generated from a small ad hoc database to a more detailed and sophisticated mechanism developed by a competent outsourced provider.

It is important to have an effective two-way reporting mechanism with top leadership for standard communications. It is crucial to have a robust and immediate mechanism for use in the event of an emergency.

The sharing and recording of lessons from incidents and near misses is a vital part of any risk management framework. The exact method by which these data are recorded and reported will depend upon the size and complexity of the organization. For example, lessons learned can be extracted from post-travel reports, combined in a database at the TRM programme level, and shared either as part of annual training or in TRM-specific reminders (these can be ad hoc or monthly, depending on the organization).

Annex A
(informative)

Development and implementation of a TRM programme

Figure A.1 describes a TRM programme in four stages. These should be integrated with any current risk management activities consistent with ISO 31000 or other risk management frameworks. The TRM programme can also be used on a standalone basis by organizations without formal risk management programmes to meet duty of care requirements.

Stage 1 helps define and integrate a TRM programme into the organization by connecting the scope and objectives set out with existing risk management activities. It focuses on the strategic aspects and sets the organization's policies. These should integrate with and complement other management activities, such as crisis management, and ensures policies, processes and objectives are clearly understood.

Stage 2 covers the key activities needed for effective risk management: identifying, assessing and determining treatment measures needed for the traveller and the organization. These activities should meet the scope and objectives in Stage 1 and be applied in Stage 3.

Stage 3 provides the processes to manage the day-to-day travel activity across the business. This stage provides the traveller and the organization with operational resources and support needed to travel while managing the risks. This stage should include clear escalation procedures if there is a serious incident affecting the traveller or the organization and this should integrate with crisis or incident management processes.

Stage 4 provides the organization with information and feedback on the effectiveness of planning and the performance of any service providers and can provide additional information from the traveller that can be useful for performance development. This information can be regularly shared with other appropriate stakeholders.

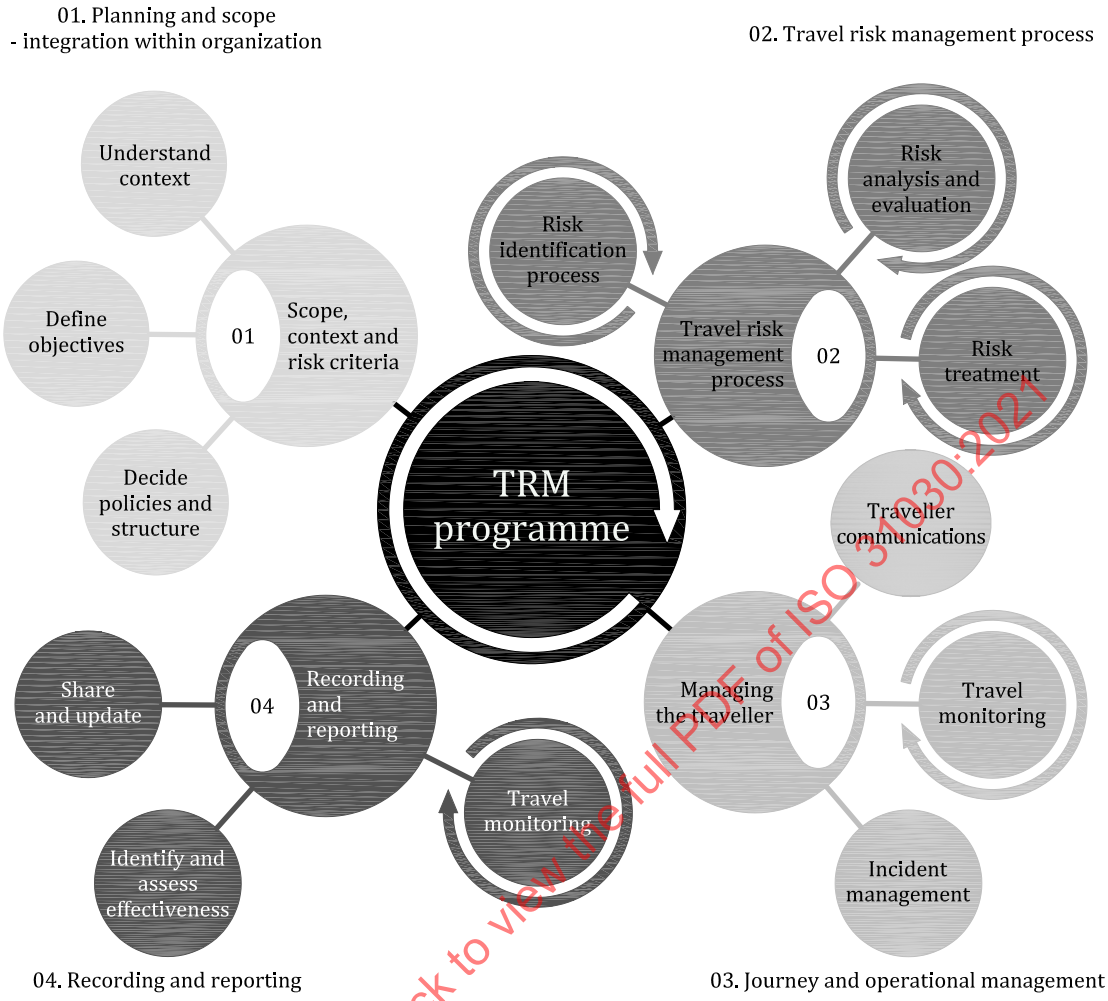

Figure A.1 — Overview of travel risk management programme

It is essential for an effective TRM programme that top management understand their duty of care responsibilities and that they are committed to supporting the programme with appropriate time and resources. Top management and other relevant decision-makers should receive regular reports and review the performance of the programme, regularly reflecting the needs of the organization and its changing needs.

Top management is responsible for ensuring that the organization has access to appropriate skills, capabilities and the appropriate reliable information necessary for effective decision-making.

Table A.1 gives an example of activities in each stage of the TRM programme. Organizations should extend or tailor these activities to fit their specific needs.

Table A.1 — Development and implementation guide

Stage one	Stage two	Stage three	Stage four
Scope, context and risk criteria	**Travel risk management process**	**Journey and operational management**	**Recording and reporting**
— Gather information on business travel, how it is managed and how it relates to the performance of the organization — Explore the travelling population to understand duty of care requirements — Conduct a gap analysis to evaluate the need for health and safety and security measures that are appropriate to the needs of the traveller and business, aligning with the organizational objectives and risk appetite criteria — Define roles and responsibilities for the implementation of the TRM programme, including stakeholder support, by preparing a business plan — Achieve stakeholder and top-level support including a provisional budget — Create a suitable management process integrated with the organization's risk, travel and governance policies — Document the process recording the decisions and supporting the rationale	— Communicate and consult with relevant stakeholders and identify and engage with those who should be involved in risk assessment or have relevant information and expertise — Conduct due diligence to ensure competent and credible internal and external suppliers — Develop and maintain a proactive risk identification process which identifies all operational and traveller specific threats and risks — Regularly analyse risks to understand their nature and characteristics including uncertainties, sources, causes and drivers of risk, consequences, likelihood, events, scenarios, controls and their effectiveness — Ensure controls for travel risk treatment are commensurate with the pervading risk and prioritize all health, safety, security and duty of care factors — Determine the competence criteria according to the roles and responsibilities assigned — Develop a mechanism whereby medical and security levels of risk for travellers, locations and operational activities can be classified — Identify and source expertise or specialist guidance that can be required to address certain special risk factors such as kidnap and ransom, and evacuation	— Implement all controls identified in the risk assessment — Prepare travellers for travel through effective training and education — Communicate risk factors to the traveller before and during travel using dialogue as well as technology — Develop a robust compliance process aligned to the defined organizational and traveller-specific risk criteria — Ensure all travel is booked through appropriate channels to ensure visibility of all planned travel — Establish either a manual or technological traveller location and communication solution — Develop and communicate changes of plan, and emergency and incident management procedures — Proactively monitor local conditions and provide traveller updates as appropriate — Ensure incident management planning is aligned to organizational crisis management planning	— Identify issues or opportunities for TRM improvement and consider changing risk treatment — Assess the effectiveness of risk treatment and review the controls in place — Produce documentation to satisfy legal, jurisdictional and regulatory requirements — Provide leadership and key stakeholders with key metrics — Ensure travel risk records and management activities/outcomes are appropriately recorded and stored — Regularly review the organization's risk management objectives and policies, updating TRM as appropriate

Annex B
(informative)

Minors travelling without legal guardians

B.1 General

Underage students or children travelling without their parents are unable to make legal decisions for themselves. This annex defines elements that should be taken into account when handling TRM for those under 18 years old (or otherwise defined as a minor by applicable national laws) and not accompanied by their parent or legal guardian (both subsequently referred to as "guardian").

This annex further refers to the duty of care of organizations with two possible scenarios: traveller (e.g. school trip) or dependent of traveller (e.g. expat or business travellers). It is intended for both international and domestic travel.

The TRM policy of the organization should cover the items described in B.2 to B.5, to be addressed in three phases: pre-travel, during travel and post-travel.

B.2 Roles and responsibilities (guardians, chaperones and organizations)

The main responsibility of guardians is to provide necessary consent and the appropriate documentation when minors need to travel without them. This consent should delegate authority and confirm the status of the parents and the acceptance of all guardians involved.

The pre-travel consent should also anticipate other situations (other than medical ones) and include them as specific things that the authorized chaperone can do for the minor (provided the applicable legislation allows it). This allows chaperones to do the necessary paperwork for the minor, thus reducing the risk of making the parents travel to where the minor is located in cases where these situations arise.

Chaperones or any other responsible adult working with minors should be competent to do so and should have a current security and safeguarding clearance.

Evidence of competence should be demonstrated through one, or a combination, of the following:

— relevant experience of activities of a similar nature;

— in-house training and assessment;

— a relevant and current national or local equivalent, or international, qualification or award.

A statement of individual competence should be provided in the form of a written statement giving:

— the name of the person to whom it applies;

— the scope of the statement;

— the name, experience and qualifications of the person making the statement;

— the criteria used to determine competence;

— the date and content of any assessment.

The organization's main responsibility is to maintain and secure the health, safety and security of the minor.

B.3 Appropriate documentation and preparation

The organization should do the following.

a) Have on file an informed consent document signed by the parents/guardians of the travelling minor(s) and contact details of the minor, accommodation, transport provider, chaperones or any other responsible adult.

b) Indicate the transportation method, service provider (if any), driver and private vehicle use. For licensed transportation providers, specific regulations concerning minors can exist in some jurisdictions. In the case of volunteer chaperones providing transportation, the organization should verify that the vehicles are in good condition and are covered by appropriate insurance.

c) Document relevant medical information concerning the travelling minors (possible limitations, medications and their administration, any waivers required; note that in some jurisdictions certain rights cannot be waived).

   It is strongly recommended that the traveller carry sufficient medication for the duration of the planned travel, plus reserve quantities in case of delays or emergencies encountered in their travels. This should include both medication they take regularly and also medication they need to take in response to irregular and unpredictable health episodes.

d) Ensure that chaperones have all proper and necessary documentation of the travelling minors (passports, visas and similar travel documentation) in their possession and the validity of the documents is sufficient for the visit.

e) Keep records for each travelling minor in a safe and secure manner and grant access to these records if required.

f) Verify that any necessary conditions of entry to the area/country, such as financial documentation, vaccination and invitation letters, among others, are complied with.

g) Ensure insurance considerations are given to the type of activity to be undertaken in order to obtain the proper insurance coverage.

h) Ensure all relevant documentation and necessary medication are secured in carry-on luggage and not in checked luggage.

i) Provide aide-memoires to the minor, in case they are away or separated from the chaperones or any other responsible adult and require assistance.

B.4 Clear and concise communications

At all times during minors' travel there should be ready access and communication between guardians and chaperones or other temporary guardians.

In situations where minors are travelling to remote areas, the organization should consider providing the chaperones access to satellite telephones.

B.5 Expenditure

The TRM policy should:

a) clarify what the organization will cover for travelling minors and define applicable procedures;

b) define procedures for specific conditions that require additional expenditure (e.g. pre-existing medical conditions which can require medications, medical equipment, medical care and training of guardians);