PETERS & PETERS

OCTOBER 2022

TRAVEL RISK MANAGEMENT STANDARD

ISO 31030

ISO 31030 Travel Risk Management

Legal implications and risks for organisations

Objectives

ISO 31030 was published in September 2021 to complement the general ISO 31000 Risk Management Standard. The ISO standard is the first truly global benchmark for travel risk management and provides a framework of good practice.

This paper aims to help corporates understand the ISO's potential implications for an employer's travel security obligations and liabilities in the context of existing UK law. Understanding ISO 31030 will help corporates whose employees are required to travel to consider the extent to which they are meeting their duty of care to their employees and others in the context of travel[1]. Nothing within this paper should be treated as legal advice, which will always vary depending on the specific situation.

> This paper aims to help corporates understand the ISO's potential implications for an employer's travel security obligations and liabilities in the context of existing UK law.

Executive summary

Below, we explore some of the UK civil, regulatory and criminal legal implications that may affect a corporate when an employee or other person suffers harm, injury or death connected to work related travel. It is critical for all businesses to understand responsibilities they owe to their employees and others, as well as the options that could be available to an employee or other person should they decide to take action against their employer, and the potential for legal action by UK regulators and public authorities.

Ideally, businesses that require their employees to travel regularly should also have proportionate, periodically reviewed and monitored compliance policies and procedures in place to help to mitigate the risk of such an incident, and to assist them in responding to any incidents that do take place.

As covered below, compliance or otherwise with the ISO standards could have a variety of potential evidential implications in civil and criminal proceedings. Companies that send employees on UK or foreign travel will want to ensure travel security risk management policies are reviewed and enforced in accordance with ISO 31030.

By way of example, and relevant to current Covid-19 travel risks, the ISO recommends in relation to accommodation selection that *"where an individual or on-site assessment is considered to be appropriate, an organization should use competent internal or external assessors"*[2]. As an industry standard developed by experienced international experts, adherence to ISO 31030 could be beneficial in demonstrating that a business has assessed and managed overseas accommodation risks to the highest possible benchmark. Non-compliance could be detrimental evidentially in a civil or criminal assessment of liability, should an employee contract Covid-19 on a work trip due to poor hotel risk management standards.

[1] The ISO identifies various duty of care requirements for different employers. For instance: direct workers, supply chain workers, interns and guests of the organisation, families and others travelling with the primary traveller, and students.

[2] See ISO31030, paragraph 7.4.5, page 20.

Summary of the key provisions in the ISO

The ISO is geared towards providing organisations and more importantly, management, with the tools to identify, assess and manage travel risks for work-related travel. This approach has been defined as "Travel Risk Management" (TRM), i.e., *"coordinated activities to direct and control an organisation with regard to travel risk"*[3]. The ISO provides a structured and comprehensive approach to formulating a TRM programme with defined objectives as well as a TRM policy.

The ISO builds on the ISO 31000 which offers a framework and process for managing risk[4] as well as ISO 45001, a standard for occupational health and safety management [5/6]. The ISO can be applied to a wide range of organisations including commercial organisations, charitable organisations and governmental and non-governmental organisations[7].

Potential relevance to civil law liability

The ISO refers to the need for an employer to be cognisant of its duty of care to its employees. It defines "duty of care" as a "moral responsibility or legal obligation of an organisation to protect the travellers from hazards and threats" and notes that:

a. A legal duty of care can arise from various sources of law.
b. Legal obligations, and how they arise, including insurance coverage, may differ between jurisdictions.
c. Legal obligations may be qualified in scope (e.g. may not be absolute).
d. Organisations should seek advice from a competent legal advisor to ascertain the scope and nature of their legal duty of care relating to the context of this standard.

Employers in England and Wales owe a duty of care in law to take reasonable care of their employees' health, safety and security during the course of their employment, even when this employment is carried out overseas. In employment contracts between the employer and the employee, this duty may be express or implied, meaning that the duty is written into the employment contract, or the court will read the duty into the employment contract.

If an employee suffers loss while working abroad, the employer may be liable if:

a. The employer owed the employee a duty of care.
b. The employer had breached that duty of care.
c. The breach of duty caused the loss and that loss is recoverable.

[3] See ISO31030, paragraph 3.20, page 4.
[4] See "ISO 31000, Risk management"
[5] See "ISO 45001 is designed to prevent work-related injury and ill-health and to provide safe and healthy workplaces".
[6] The ISO advises that "As such, elements of this document can assist or inform organizations developing such management systems, but it is not a management system standard", see ISO 31030, Introduction, page vi.
[7] The ISO does not apply to tourism and leisure-related travel, except in relation to travellers travelling on behalf of the organisation.

Who owes the duty of care?

The ISO and the law of England and Wales are clear: top management should be responsible and accountable for the overall implementation of policies to reduce the risks to employees associated with travel overseas. If they do not take such responsibilities seriously, this may lead to corporate as well as personal liability.

The corporate employer

The employer's duty of care to their employee is personal and non-delegable. It would therefore be a misconception for an employer to believe that they can engage the services of a third party to negate the risk of liability completely. Consequently, while it may be reasonable for an employer to contract with a travel management company in respect of arrangements for their employees, the employer will not be excused for the travel management company's failures if it should have known of them.

Similarly, an employee's secondment to a third party will not mean the employer is absolved of responsibility for that employee's safety and security. For instance, an employee was injured in a roadside bombing while working abroad on a contract between his employer and the Ministry of Defence.[8] The Ministry of Defence accepted that it owed the employee a duty of care and had assumed a responsibility to keep him safe. However, the Court confirmed that this did not release the employer from its own liability if the duty to take reasonable care was not fulfilled by it and the Ministry of Defence between them.

A company is a legal person, distinct from its directors and shareholders. Therefore, liability for breaches of duty to the company's employees generally rests with the company, with which the employee has contracted. However, this is not to say that directors of the company or its parent(s) cannot incur liability.

Directors

General duties are owed by a director of a company to the company. Many of these duties have been codified by the Companies Act 2006. Section 172 of the Act requires directors to promote the success of the company. As part of that duty, and as set out by section 172(1)(b), a director is required to act in the way he considers, in good faith, would be most likely to promote the success of the company and in doing so have regard to the interests of the company's employees. Section 174 of the same Act imposes a duty on the director to exercise reasonable care, skill and diligence.

The general principle is that directors of a company will be liable for the torts of the company, committed at their direction.[9] For instance, if a director of a company knows that boats operated by his company are defective, but chooses not to take any action and, as a result of a defect, an employee falls overboard injuring himself, the director will be personally liable to the employee.[10]

Parent companies

If a parent company exercises control over the subsidiary's activities, it may then owe an independent duty of care towards employees of the subsidiary. The liability of a parent company for the acts of its subsidiary has been examined extensively in the case law.[11] The key question is one of proximity: whether what the parent company did amounted to taking on a direct duty to the subsidiary's employees. Circumstances in which the law could impose responsibility on a parent company for the health and safety of its subsidiary's employees include:

If a parent company exercises control over the subsidiary's activities, it may then owe an independent duty of care towards employees of the subsidiary.

[8] *Hopps v Mott MacDonald Ltd* [2009] EWHC 1881 (QB)
[9] *Rainham Chemical Works v Belvedere Fish Guano Company Ltd* [1921] 2 AC 465
[10] *Yuille v B&B Fisheries (Leigh) Ltd (The Radiant)* [1958] 2 Lloyd's Rep. 596
[11] See in particular *Vedanta Resources Plc v Lungowe* [2019] UKSC 20 and *Okpabi v Royal Dutch Shell Plc* [2021] UKSC 3

a. The businesses of the parent and subsidiary are in a relevant respect the same.
b. The parent has, or ought to have, superior knowledge on some relevant aspect of health and safety in the particular industry.
c. The subsidiary's system of work was unsafe, as the parent company knew, or ought to have known.

What is reasonable care?

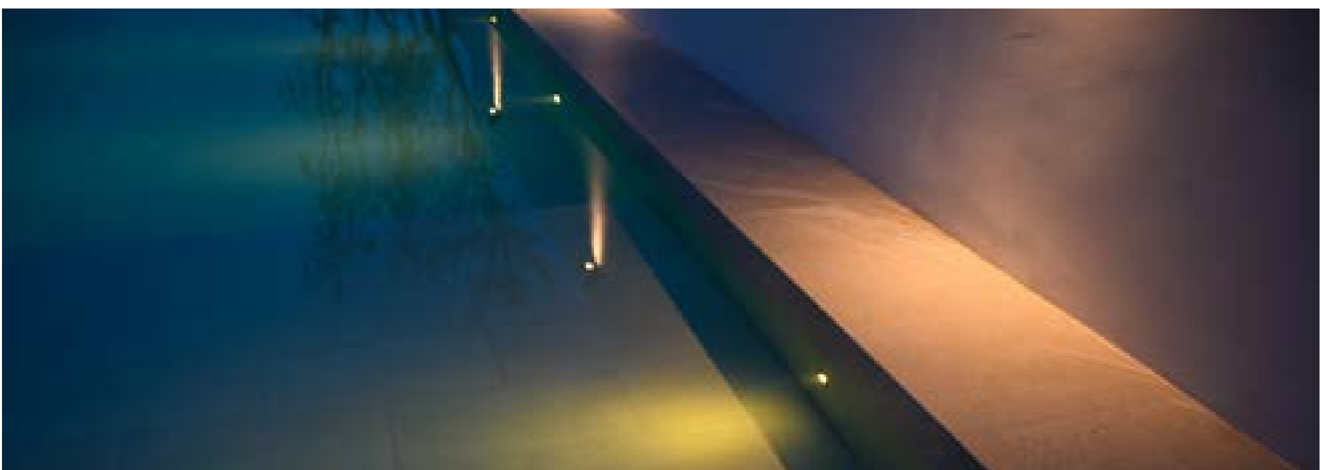
When determining what a reasonable employer should have done, the court will have regard to the standard prevailing in the relevant jurisdiction at the time, which is usually proven by way of expert evidence. However, the Courts have demonstrated time and again that a person's adherence to recognised professional standards or industry accepted standards will tend to suggest they have behaved reasonably. Further, if there is no local standard, the court may use generally accepted professional standards to fill the void.

For instance, in *TUI UK Ltd v Morgan* [2020] EWHC 2944 (Ch), the appellant tour operator, unsuccessfully appealed against a decision that it was liable to a holidaymaker for injuries sustained at a hotel in Mauritius during a package holiday. The holidaymaker had suffered injury when she collided with a heavy wooden sunbed while walking back to her room after dinner along an unlit sun terrace.

There was no prevailing local standard for lighting in Mauritius and the High Court held that the judge at first instance had been entitled to rely on International Standards Organisation's ISO 30061 on emergency lighting. Even though the ISO standard applied to minimum luminosity requirements for installed emergency lighting and did not prescribe what areas were to be lit, so was not directly applicable to the accident site in this case, the question before the judge was not whether that standard was applicable, but whether it was an appropriate standard to use to determine the factual question of whether the tour operator had breached its duty to perform the services it was providing to the holidaymaker with reasonable skill and care.

On causation (which will be explored further below), the appeal court held that the judge had been entitled to infer that, had the minimum standard described in the ISO Standard been met, the holidaymaker would have been able to see where she was going. The whole point of the emergency lighting in the Standard was to enable the ordinary person to navigate areas so lit safely. Even that minimum standard might be insufficient to enable some individuals to find their way, but the judge had been entitled to proceed on the basis that the holidaymaker had the visual acuity of the ordinary person.

When determining what a reasonable employer should have done, the court will have regard to the standard prevailing in the relevant jurisdiction at the time.



Risk assessments

As a general rule, the ISO states that travel should be considered as part of a risk assessment process. This process should include risk identification, risk analysis and risk evaluation.

Employers' duties to carry out risk assessments were considered in *Dusek v Stormharbour Securities LLP* [2015] EWHC 37 (QB) and *Cassley v GMP Securities Europe LLP* [2015] EWHC 722 (QB). *Dusek* and *Cassley* had similar fact patterns but were decided differently by the Court.

In *Dusek*, an employee was required to fly by helicopter across the Andes. Notwithstanding the turbulent weather, the crew decided to make the return trip and crashed, killing all on board. The Court found that the employer, an English LLP, owed a duty to take reasonable care to ensure that the employee was safe while travelling to and from work overseas. Given the obvious potential dangers in the trip, the employer owed a duty to inquire into its employee's safety and to conduct a risk assessment. The Court found that had the employer conducted a proper risk assessment, the company would have advised its employee not to take the flight. By taking no steps at all, the employer had breached its duty of care.

In *Cassley*, an employee was killed when a private charter flight crashed in the Republic of Congo, en route from Cameroon. A duty of care was owed, as travel on private charter flights was an essential part of the employee's work. The Court found that the employer had breached their duty of care by failing to undertake sufficient enquiries into the safety of the flight.

However, the carrier transporting the employee had been changed at the last minute, which the employer had no way of knowing. If the employer had made enquiries, it would have been about the original carrier, which was reliable and appropriate. As a result, in the counterfactual (i.e. in a scenario where the employer had undertaken sufficient enquiries), the employer would not have prevented the claimant from boarding the flight. Therefore, even if the employer had conducted the risk assessment, the employee would have boarded the flight.

Causation and recoverability

The case of *Cassley* shows that, when determining liability, the Court will ask what the employer should have done (the counterfactual) and whether this would have resulted in a different outcome. If the employer's actions in the counterfactual would have made no difference to the loss suffered by the employee, the employer may be found in breach of duty, but will not be required to pay compensation.

Similarly, if the consequence of a person's actions are not reasonably foreseeable, it is unlikely that anyone can be held responsible for the damage suffered as a result. If the consequence of a person's actions are reasonably foreseeable, the court will still ask whether the damage is too remote because it has been caused by a break in the chain of causation (or a novus actus interveniens). If the person's actions were unreasonable, or the conduct was voluntary, independent, deliberate and informed, the court is unlikely to find that the breach of duty caused the damage claimed.[12] Employers will expect their employees to act responsibly whilst on work trips. However, a court will consider causation in light of all the facts. Where a hotel or other third party has exhibited clear failings and an employer has not conducted a risk assessment (or delegated anyone to do this for them), this could lead to the employer being found liable.

An example of a novus actus interveniens is found in *Clay v TUI Ltd* [2018] EWCA Civ 1177. In *Clay*, a man sustained injuries as a result of falling from a hotel balcony.

> If the consequence of a person's actions are not reasonably foreseeable, it is unlikely that anyone can be held responsible for the damage suffered as a result.

[12] *Spencer v Wincanton Holdings Limited* [2009] EWCA Civ 1404

Having found himself stuck on the balcony because of a malfunctioning lock on the balcony door, the man attempted to climb to a neighbouring balcony. The Court found that the man's conduct in doing so was so unreasonable in the circumstances that it broke the chain of causation.

By contrast, in *Al-Najar v Cumberland Hotel (London) Ltd* [2019] EWHC 1593 (QB),[13] the High Court held that a London hotel was not liable for serious injuries sustained by three guests who were violently attacked in their room by an intruder who gained access after the guests left their door on the latch. The Court found that the hotel's duty of care did extend to a duty to protect against injury by third parties and the attack by the third party did not amount to a novus actus interveniens on the basis that the attack was foreseeable, if unlikely. The court heard evidence from experts (on both sides) in security operations and security risk management. Having regard to this, the Court found that the evidence as a whole showed that the hotel took security seriously and that they took reasonable care to protect guests against the injuries caused by attackers. Whilst some of the additional measures suggested might have prevented the attack, it was not possible to say that it was more likely than not that they would have prevented it.

The ISO recommends that assessing and selecting accommodation be included as part of an organisation's travel risk management policy. Under common law, an employer must protect workers and others such as contractors from risks to their health and safety. In the context of business travel, an employer should be aware of the standards of accommodation varying from country to country and equally, an employee should expect to stay in accommodation which does not present any health and safety concerns. As stated in *Cassley* however, the emphasis is on a duty not to expose an employee to foreseeable unnecessary risks in the course of work-related travel. As a result, an employer is likely to be expected to carry out some form of risk assessment of accommodation based on the individual circumstances.

[13] Upheld on appeal in [2020] EWCA Civ 1716

[14] *See Palfrey v Ark Offshore Ltd* [2001] 2 WLUK 699 which has a similar fact pattern.

Case study

An engineering company based in the UK asks its employee to travel to West Africa to advise on the extent of repairs that should be made to equipment on an oil rig operated a client. The client gives assurances they will take responsibility for the employee and arranges flights, accommodation, security and transport. Because of these assurances, the employer does not make enquiries about the location and does not carry out any risk assessment.

Before travelling, the employee asks one of the directors of the employer (Director A) whether he needs any vaccinations. The director replies that the employee does not need any vaccinations as he will be based offshore. The director knows this information to be untrue, but suspects it is too late for the vaccinations that the employee needs to take effect and does not want to lose the contract with the client.

Upon return to the UK, the employee dies from malaria and his widow sues the employer on the basis that it had not warned her husband of the risks of tropical diseases abroad and did not provide him with anti-malarials. She also sues Director A personally.

It is likely that, in this scenario, both the company and Director A would be found liable for the death. The Court would likely find that the absence of an effective policy for warning employees of the risks of tropical diseases abroad would be a breach of a duty to take reasonable care to ensure the safety of employees in the course of their employment.[14]

The Court is also likely to look unfavourably on the failure to carry out a risk assessment, which would have highlighted the risk of malaria. As previously mentioned, this would be dealt with by way of expert evidence provided by a suitably qualified expert whose evidence would refer to internationally accepted norms and industry standards for risk assessments such as the ISO. As the duty to the employee is non-delegable, the fact that the client agreed to take responsibility will not negate liability. This is particularly so in circumstances where the employee should have been vaccinated before travel (and so before the client took responsibility for him).

Director A will likely be held liable to the employee's widow on the basis that he assumed personal liability to the employee when he knowingly gave false information as to the need for vaccination. Director A would also be liable to the company on the basis that he breached his duties to it.

Potential relevance to criminal law liability

The Health and Safety at Work Act 1974

Under UK criminal law, the Health and Safety at Work etc. Act 1974 ("HSWA") sets out the broad health and safety duties of a company and its directors, managers and employees[15] for ensuring that employees and non-employees are not exposed to risk from work activities in the UK insofar as is "reasonably practicable". The Act extends to foreign companies that have a UK branch or place of business[16] and to overseas workers in the UK, however it has limited reach for events which take place outside of the UK or its territories.

The Act requires employers to have in place adequate systems which are followed by employees. In assessing whether such adequate systems are reasonably practicable, as is required by the Act, the extent to which danger is foreseeable should be weighed against the possible measures that could mitigate or eliminate it, including the costs involved. If the risk is small but the measures required would be very significant, a company may be exonerated. A company will not be able to escape liability by showing that it has taken steps at a senior level if all reasonably practicable steps have not been taken at an operating level. Individual members of staff can also be charged with HSWA offences.

Even if no actual harm is caused, a company could be guilty of an offence. For example, if a hotel reopens after a pandemic-related lockdown but fails to take adequate precautions to deal with ongoing infection risks, it could in principle be prosecuted even if no one is harmed. For an employer using that hotel, compliance or non-compliance with ISO 31030 is likely to be an evidential factor taken into account when assessing whether adequate and reasonably practicable systems and procedures have been adopted.

Under section 37 HSWA, a criminal offence can be committed by a director, manager, secretary or other similar officer, if it is proved that they consented to or connived in a criminal offence by the relevant body corporate, or if the offence was attributable to their neglect.

A company will not be able to escape liability by showing that it has taken steps at a senior level if all reasonably practicable steps have not been taken at an operating level.

[15] The HSWA 1974 is also supported by a suite of health and safety regulations.

[16] See HSE, "Prosecution of foreign defendants"

[17] See ISO31030, paragraph 5.6 (d), page 12

Case study

A French mining company has sent a group of geologists to take soil samples from an excavation site in the north of England. It has been raining heavily in the area and is due to rain more, which the employees were not informed about. The company does not have a risk assessment procedure in place to ensure that the excavation pits are safe to work in. While one of the employees is working in the excavation pit, it begins to collapse due to significant flooding. His colleagues become panicked and are unable to contact their team leader, based at the UK branch of the company in London as they are on annual leave having forgotten about the trip. The employee suffers serious injuries and his family, with the support of the local MP and newspapers, urge the Health and Safety Executive ("HSE") and local police force to take action.

This case study highlights the importance of incident management planning. The ISO recommends appointing a competent person to be responsible for crisis or incident management and developing procedures to communicate urgently in connection with safety, security or health matters. Typically, this would involve a designated emergency contact point available at any time from where they are located, and specific escalation protocols[17]. The HSE may well have regard to failings in this regard when weighing up whether the mining company should be charged with a HSWA offence. The team leader may also be at risk of being prosecuted for consenting and conniving in the company's offence under section 37.

Corporate manslaughter

The UK's corporate manslaughter offence was created by the Corporate Manslaughter and Corporate Homicide Act 2007 ("CMCHA"). It applies to UK corporate entities and foreign incorporated entities operating in the UK. An organisation will be guilty of the offence if all of the following criteria apply:

a. the way in which its activities are managed or organised causes a person's death;
b. the death results from a gross breach (meaning conduct which falls far below what can reasonably be expected of the organisation in the circumstances) of a relevant duty of care owed to that person; and
c. the way in which senior management managed or organised the organisation's activities forms a substantial element of the breach.

Where it is established that an organisation owed a relevant duty of care to a person and it falls to the jury to decide whether there was a gross breach, the CMCHA includes certain factors that a jury must consider, specifically whether the organisation failed to comply with health and safety legislation (including the HSWA) that related to the breach, and if so:

a. how serious the management failure was; and
b. how much of a risk of death it posed[18].

ISO 31030 is a guidance standard only at present. Whilst adherence or not with the standard is unlikely to be definitive per se when considering whether a gross breach of a duty of care has taken place sufficient for a corporate manslaughter offence, it is highly likely to have evidential value in relevant circumstances.

If a death occurs in the UK, the UK courts will have jurisdiction even if the breach of duty from which the harm resulted occurred abroad or if the company itself is foreign incorporated[19]. The UK courts will not have jurisdiction in cases where the relevant harm took place abroad, unless this occurred in the UK's territorial waters, on a British ship, aircraft or hovercraft, or on an oil rig or other offshore installation already covered by UK criminal law[20]. In that case however, there are likely to be local laws that attach legal liability within the jurisdiction of the death.

Organisations should be keenly aware of the offence of corporate manslaughter not least because it carries large penalties, potentially including an unlimited fine based upon a significant percentage of turnover.

[18] Section 8 of CMCHA 2007
[19] Ministry of Justice, A Guide to the Corporate Manslaughter and Corporate Homicide Act 2007, page 17.
[20] Ministry of Justice, A Guide to the Corporate Manslaughter and Corporate Homicide Act 2007, page 17

Case study

A Danish software company has sent an employee to attend a meeting with local partners in Reading, England. The employee has a serious allergy to peanuts which they highlighted to the employer in writing during the booking process for their accommodation abroad, asking the travel manager to pass this on to the hotel's catering team. The travel manager confirms that this will be done, but no internal note is made of the allergy, and it is not communicated to the hotel. The travel manager has previously rebuffed attempts to have a policy around allergies on grounds that it will encourage "people being fussy". The hotel staff do not ask the employee if they suffer from any allergies. The employee is exposed to peanuts at dinner at the hotel, suffers from an attack, and dies. Their family members share their grief and outrage on the news and social media, leading to media scrutiny.

The company could well find itself under investigation for corporate manslaughter in the UK. An investigator would consider a number of factors, including any health and safety guidance relating to the breach and whether there were any attitudes, policies, systems or accepted practices in the organisation that were likely to have encouraged a management failure. ISO 31030 states that arrangements to reduce risk should be continually monitored and reviewed, including mitigation of medical and health risks. The ISO recommends that organisations should consider appropriate checks for all travellers to ensure they are medically fit for planned travel and should ensure that the destination country can medically support any traveller with pre-existing conditions should a health

incident occur. Failure to comply with the standard may well be a factor which bereaved families / media draw out to the company's reputational detriment. It may also be a relevant decision-making factor for a prosecutor or court.

If the death occurred abroad (other than as described above, notably "abroad" in this context excluding UK territories such as BVI or Gibraltar), the company could not be pursued under the UK corporate manslaughter offence. However, local law enforcement agencies are likely to consider investigating, especially where, for example, bereaved relatives and media apply pressure. In that instance, a UK company would want to retain local counsel to advise, which can often be best managed through UK legal advisers. The common law offence of gross negligence manslaughter applies to individuals and does extend to deaths that occur abroad. It is feasible that any particularly culpable individual, such as the travel manager in this scenario, could be at risk of prosecution.

Inquiries and inquests

Inquests involve the investigation of the circumstances surrounding the unnatural death of one or more individuals. Where a fatal workplace accident has occurred in the UK, the death must also be reported to the local Coroner, who is under an obligation to conduct their own investigation into how the death was caused. Coroners in England and Wales also have a duty to inquire into a death that occurred overseas if the body has been repatriated and under particular circumstances[21/22]. Public inquiries have a broader discretion to consider a wider range of issues and are generally reserved for significant events of public importance.

If an inquest or inquiry were called into a travel-related death, it is highly likely that the ISO standards would be referred to as having evidential weight to either support or detract from a corporate's position.

Case study

A UK travel company organises guided hiking excursions abroad and has decided to begin offering a picturesque hiking tour in a new country. No security audit or assessment is undertaken to identify any potential travel risks. On one of the new expeditions, the group of hikers with the guide are stopped by an armed local militant group that demands money in exchange for safe passage. The guide refuses to pay the group and they kill all members of the hiking group.

The above case study echoes some of the legal issues raised in the terrorist attack carried out in Sousse, Tunisia in June 2015, which resulted in the deaths of 38 tourists following an attack on their resort. The inquest heard that a travel company did not carry out frequent security risk assessments on resorts or hotels before the atrocity took place[23]. The Judge-Coroner who investigated and led the inquest into the deaths of the 30 British nationals concluded that all of the victims were unlawfully killed[24] and expressed concerns that prior to the attack, related travel companies did not have security advisors on their boards.

The ISO explains that *"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."*[25] Travel risk assessments should cover both security threats and health and safety hazards.

The ISO standard provides a means for organisations to demonstrate that travel decisions are based on the organisation's capacity to treat risk using internal resources or with external assistance. Not all travel warrants the same level of rigour for risk assessment and management, and organisations should be careful not to let commercial goals take precedence where travel is not appropriate.

[21] *R v West Yorkshire Coroner, ex parte Smith* [1983] QB 335
[22] Section 1 of the Coroners and Justice Act 2009
[23] See *The Guardian*, 19 January 2017, "Sousse attach inquest: security audit by Tui could have saved lives'"
[24] See Serjeant's Inn, UK Iquest law blog, 2 March 2017, "Tunisia Sousse Inquests conclusions are returned"
[25] ISO31030, Introduction, page vi.

Financial institutions

The Financial Conduct Authority's ("FCA") Principle 2 requires regulated firms to conduct their business with due skill, care and diligence. FCA Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems. According to SYSC Senior Management Arrangements, Systems and Controls Rule 3.1.2G, the nature and extent of the systems and controls a firm will need to maintain under SYSC 3.1.1R[26] will depend on a variety of factors including:

a. The nature, scale and complexity of its business;
b. The diversity of its operations, including geographical diversity;
c. The volume and size of its transactions; and
d. The degree of risk associated with each area of its operation.

Although the FCA's regulatory purview is focussed on protecting consumers, depending on the relevant business operations, certain regulated entities might consider including travel risks in their systems and controls (which are regularly assessed in accordance with regulatory requirements) to manage employee travel to high-risk locations.

[26] A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business.
[27] ISO31030, paragraph 4.5, page 8
[28] ISO31030, paragraph 5.5 (h)(2)(vi), page 11

Case study

A large UK bank has various branches across the world, including one branch in a high-risk jurisdiction for bribery, corruption and security issues. One of its senior managers is sent to visit the local branch to support ongoing assessment processes and procedures relating to anti-money laundering systems and controls. The senior manager books a hotel that has not been vetted by the bank independently and successfully claims the sum spent back without going through the bank's usual travel agency and approvals process. During her stay, a laptop containing sensitive personal information regarding retail customers is stolen from her locked, empty hotel room. It later emerges that access cards for the room had not all been collected from previous guests, and that no standard card wiping or monitoring system was in place to prevent former guests from accessing locked rooms after the end of their stay.

The scenario illustrates how various issues associated with operating in high-risk jurisdictions can arise. The FCA sets out in SYSC 13.7.9 that "a firm should understand the effect of any differences in processes and systems at each of its locations, particularly if they are in different countries, having regard to the business operating environment of each country as well as whether the risk management structures of the overseas operation are compatible with the firm's head office arrangements". It is unclear whether the FCA would have regard to compliance or non-compliance with the ISO guidance in the above scenario. However, the ISO similarly specifies that "The nature and scale of an organization's travel risk will inform how they are managed and delivered. The risk profile of an organisation with occasional travel to low-risk locations is very different to one operating frequently in high risk locations"[27]. This means that entities will have to adapt their systems and controls in relation to their travel and operational risk profile (which, for regulated firms, will be in keeping with the FCA's proportionate approach described above).

The ISO also highlights that in developing their travel risk programme, an organisation should list the categories of risk that can affect the organisation, including the traveller, such as risk to data and information[28]. This approach may be worth considering where travel risk is considered as part of regulatory risk assessments, monitoring and systems and controls.

For further information, please contact Michael O'Kane, Senior Partner, Peters & Peters Solicitors LLP, on mokane@petersandpeters.com, +44 (0)207 822 7755

Team members

Andrew Wallis
Email: awallis@petersandpeters.com
Tel: +44 (0) 207 822 7781

Cécile Nicod
Email: cnicod@petersandpeters.com
Tel: +44 (0) 207 822 7747

Emma Ruane
Email: eruane@petersandpeters.com
Tel: +44 (0) 207 822 7759

Julia Steinhardt
Email: jsteinhardt@petersandpeters.com
Tel: +44 (0) 207 822 7731

The purpose of this paper is to provide general and provisional thoughts on the new ISO 31030. This paper was prepared by Peters and Peters Solicitors LLP, but does not reflect the view of the law firm in the context of any particular situation or matter. The guidance set forth in the paper is for informational purposes only, and is subject to change in light of future developments in this new area. Neither this publication nor Peters and Peters Solicitors LLP are providing legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of any client relationship. The information contained within this publication is believed to be accurate and correct at the time of writing but this document does not constitute legal advice. Legal advice will always be dependent upon the specific facts of any matter and no reliance should be placed upon this document or the information contained therein. We disclaim any and all liability for any errors in or omissions contained in this document. *All rights are reserved.*

©2022 Peters & Peters Solicitors LLP