



“C’est la vie?”

**A step-by-step guide to building a
travel risk management program**

Executive Summary

Few organizations to date have developed a dedicated, fully mapped travel risk management strategy, yet understanding and mitigating such risks is extremely important for both traveling employees and their employers.

Risks for the traveler

Travel is inherently risky because it places employees in unfamiliar and/or disadvantageous environments. Examples include:

- Standing out from the local population
- Driving in unfamiliar locations and conditions
- Fatigue
- Unfamiliarity with local health risks and medical facilities

Risks for the employer

If travelers come to harm, their employers face potentially severe consequences both legally and financially, as well as to their reputation.

Understanding and mitigating risks is extremely important for both traveling employees and their employers

What is more, risks will continue to grow as companies increasingly globalize their operations. In spite of this increased exposure, organizations typically fail to start actively managing travel-related risk until a serious incident affects one of their travelers.



The findings of the white paper include:

- Travel risk management will assume increasing importance.
 - > **Evaluation** – Ratings agencies are beginning to evaluate companies' risk management performance on behalf of investors.
 - > **Duty of care** – Organizations' duty of care towards employees is expected to become increasingly enshrined in punitive legislation.
- There are six broad categories of corporate travel-related risk:
 - > Risk to personnel (health, safety and security)
 - > Reputational risk
 - > Risk to data/equipment
 - > Legal risk
 - > Financial risk
 - > Risk to productivity/trip effectiveness
- Although risk management generally is assuming increasing strategic significance within organizations, coordinated management of risks relating specifically to travel receive little attention. Liaison between the relevant departments – such as security, travel, human resources and legal – is poor.
- Two types of third-party assistant – travel management companies and travel security specialists – are essential to providing and coordinating risk management tools and processes.
- Advito proposes six steps to building a travel risk management program:

- 1 **Assign management responsibility** – Four key stakeholders are involved: initiator, senior sponsor, stakeholder with accountability, project manager. They must coordinate and motivate all relevant departments, including travel and security (where it exists), and outsourced third parties.
- 2 **Determine risk types** - Create a matrix of risk types specific to your organization.
- 3 **Assess risk exposure** - Assess your organization's capability to manage travel risks effectively and develop the risk-type matrix by plotting your organization's exposure to specific threats.
- 4 **Mitigate or manage** - Tools include:
 - **Process** – recruitment assessment; automated response at booking stage; traveler tracking system; traveler profiles
 - **Process/Information** – policy
 - **Information** - security tips; destination information, training and education
 - **Planning** – crisis management
 - **Risk transfer** – insurance; medical assistance
- 5 **Communicate** – Make travelers aware of the program and their responsibilities.
- 6 **Audit** – Monitor the success of the program and adapt it to rapid changes in the risk environment and your profile.

Case studies in the white paper include:

- **Hewitt Associates** – Serious about risk; serious about travel risk
- **DuPont** – Managing security globally in a concerted manner
- **PricewaterhouseCoopers UK** – Risk management at point of booking
- **The Capital Group of Companies** – Working with the travel management company and third-party security provider
- **ING** – Keeping travelers informed

Introduction

A crucial yet overlooked subject

“C’est la vie” – such is life – is a phrase typically uttered with a casual shrug when plans, activities or routines get up-ended or go awry. But when things go wrong for business travelers, who face heightened security, safety and medical risks whenever they leave the familiar environs of their usual work place, the consequences can be far more difficult to accept or tolerate philosophically.

Their employers also face risks related to travel. If personnel come to harm, there could be severe consequences – both legally and financially, as well as to the firm’s reputation. Travel also engenders other, less obvious, potential risks not related to duty of care, such as loss of commercially sensitive data, misbehavior by personnel and failure to limit greenhouse gas emissions.

Yet in spite of all those things that can go wrong, in spite of increased business travel to long-haul destinations and in spite of growing attention to risk management generally, management of travel-related risk has frequently been overlooked at the corporate level. Most security managers have little experience in dealing with travel risk, while travel managers are often aware of the issue but are unsure how to initiate a successful Travel Risk Management (TRM) program.

Manage risk proactively – not when it’s too late

This white paper aims to plug these knowledge gaps, and is therefore aimed at both security and travel managers. The intention is to help them take a proactive, coordinated approach to travel risk, rather than only reacting once incidents have happened.

To date, literature on this subject has been limited. A Risk Maturity Management Model from the United States’ National Business Travel Association (NBTA) and iJET Intelligent Risk Systems provides some excellent theoretical modeling. The Project ICARUS duty-of-care toolkit from the Institute of Travel Management (U.K.) includes some practical tips, especially for small and medium enterprises.

Once established, a travel risk management program addresses the “care” aspect of a broader Responsible Travel

Management strategy that also includes other dimensions of Corporate Social Responsibility (CSR), including environmental sustainability. (For more information on Responsible Travel Management, download the *2008 NBTA CSR Toolkit 2008* powered by Advito for free from www.advito.com).

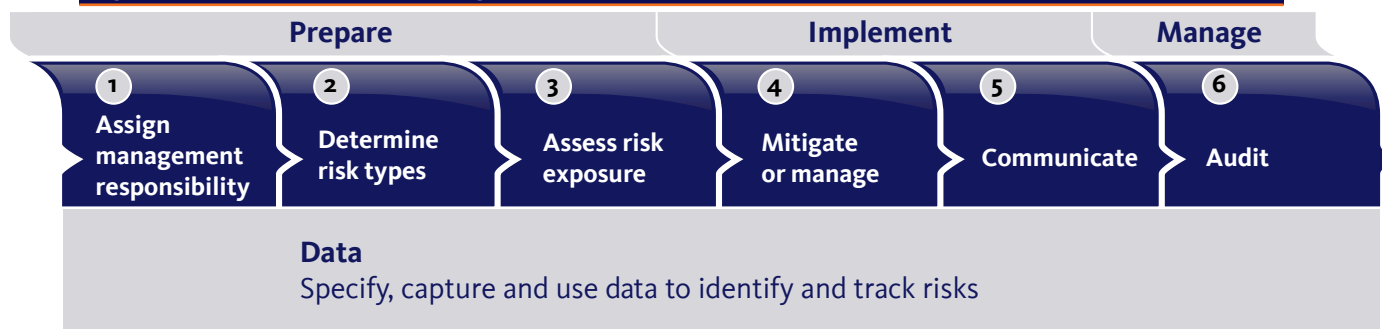
This paper sets out a beginner’s guide to the “what,” “why” and, above all, “how” of travel risk management, including a step-by-step strategy for putting together a TRM program.

Broadly speaking, the range of risk types relating to corporate travel is as follows:

Risk to personnel	Security (crime/civil unrest) Security (terrorism) Safety Health (illness) Health (stress)
Risk to reputation	Failure in duty of care to employees Carbon footprint Misuse of travel expenses Unethical conduct by travelers
Risk to data/equipment	Protecting data carried by employees while traveling Protecting data collected about employee travel Lost, stolen or damaged baggage, equipment and personal items
Legal risk	Duty of care/health & safety legislation Data protection regulations Failure to comply with tax laws Illegal activity by travelers
Financial risk	Financial penalties of exposure to legal risk Misuse of travel expenses
Risk to productivity/trip effectiveness	Lost, stolen or damaged baggage, equipment and personal items Inadequate technology/support for travelers Failure to meet immigration requirements

For the purposes of this white paper, Advito proposes a simplified model to help organizations start a Travel Risk Management program:

Fig 2. Simplified Travel Risk Management model



1 Assign management responsibility

- Travel Risk Management involves a cooperative effort from numerous departments and functions, including travel management, security, HR, legal and medical.
- Stakeholders are required to drive the strategy within four different roles: initiator, senior sponsor, stakeholder with accountability, project manager.
- Smart outsourcing provides crucial aspects of the Travel Risk Management program unavailable internally in terms of expertise, intelligence, technology, resource and impartiality. Key third parties are specialist travel security providers, travel management companies and medical assistance organizations.

2 Determine risk types

Create a matrix of risk types specific to your organization. The matrix in Figure 1 can be used as a template.

3 Assess risk exposure

- Strategic – Assess your organization’s capability to manage travel risks effectively, e.g., by using the NBTA/ iJET Risk Management Maturity Model and/or involving a specialist advisor.
- Tactical – Develop the matrix in Figure 1 to plot your organization’s exposure to specific threats.

4 Mitigate or manage

- Each identified risk can be mitigated or managed through one or more basic techniques: Treat, Transfer, Terminate, Tolerate.
- Tools used specifically for management and mitigation of travel risks include:
 - Process* – recruitment assessment; automated response (e.g., triggering of approval requirement) at booking stage, traveler tracking system, traveler profiles
 - Process/Information* – policy
 - Information* - security tips, destination information, training and education
 - Planning* – crisis management
 - Risk transfer* – insurance, medical assistance

5 Communicate

Having a Travel Risk Management program is not enough. Travelers must be made aware of it and of their responsibilities.

6 Audit

- Techniques for monitoring and ensuring the continuity of the Travel Risk Management program include:
 - Creating a multi-disciplinary Travel Risk Management steering group.
 - Benchmarking regularly against best practices and peers.
 - Seeking input from senior management on likely new destinations.
 - Collating traveler feedback on risk-related issues.
 - Reviewing policies and procedures when incidents happen.
 - Ensuring policy compliance remains high.

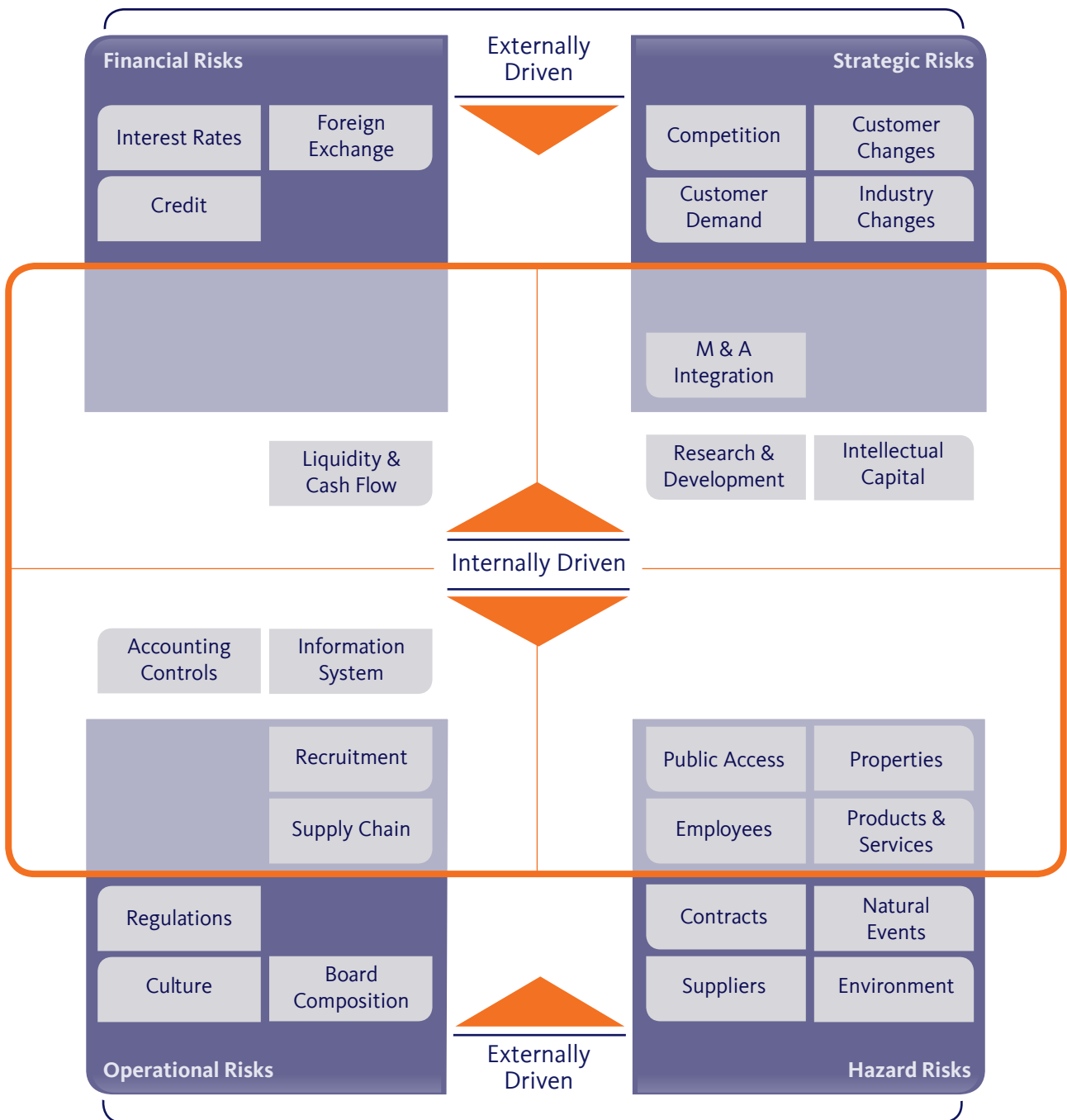
Section A

The connection between risk management, duty of care and corporate travel

What is risk management?

Risk management is the process by which an organization identifies, evaluates and mitigates or manages anything that may impact the continued success of the entity.

There are numerous types of risk. One model places them in four categories: financial, strategic, operational and hazard. It then divides each category into external and internal sub-types, as shown below:



Source: IRM, AIRMIC, ALARM

A hot topic

Organizations increasingly view their operations through the prism of risk management because failing to deal with risk poses serious threats to their continuity. These threats include:

- **Evaluation** – In Q3 of 2008, Standard & Poor's started to include evaluation of companies' enterprise risk management in its ratings. In consequence, companies will now be assessed formally by investors on the strength of their risk management. With the global economic crisis that started in summer 2007 having arguably been precipitated by poor financial risk management on the part of financial institutions, risk is currently regarded as supremely important in corporate life.
- **Duty of care** – The legal duty to protect the health and safety of employees has gained an increasing profile owing to legislation such as the Corporate Manslaughter and Corporate Homicide Act, which took effect in the U.K. in 2008. Companies fear severe penalties if they cannot demonstrate compliance through an effective risk management strategy.
- **Recruitment and retention** – Even in the current economic downturn, companies can find it hard to recruit high-caliber staff, such as engineers. Those firms that demonstrate good duty of care are seen as more attractive employers.

As a result, many large organizations and even some smaller ones now have an internal risk management group to deal with these issues. A few are going further and appointing chief security or risk officers to coordinate the many different departments that deal with risk but may not talk to one another effectively.



Some companies are going further and appointing chief security or risk officers to coordinate the many different departments which deal with risk but may not talk to each other effectively

Section A

The connection between risk management, duty of care and corporate travel



As businesses globalize, risks are becoming more acute, since travelers are increasingly likely to travel greater distances to environments less like their own

The relevance of risk management to travel

Corporate travel is inherently risky because it puts employees in unfamiliar and/or disadvantageous environments. Examples (and there are many hundreds of others) include:

- Visiting destinations where travelers stand out from the local population and may be targeted for criminal or terrorist purposes
- Driving where local laws (different side of the road), customs (not observing traffic signs) and conditions (poor-quality roads) may all be different
- Fatigue
- Unfamiliarity with local health risks (which can be greater than or different from those at home) and medical facilities (often less equipped than at home)

As businesses globalize, these risks are becoming more acute, since travelers are increasingly likely to travel greater distances to environments less like their own. However, it is important to view risk management as an enabler of travel, not an inhibitor. Business travel is possible to almost any destination in the world so long as steps are taken to mitigate the risks. Example: Without risk mitigation, it would clearly be impossible to visit the oilfields of southern Iraq. With risk mitigation, including a crisis management plan, a full destination briefing, close protection (if deemed appropriate), etc., such a trip would be possible.

Expatriates

In the context of risk, travel should include long-term expatriate assignments as well as short-term transient travel. For this group of employees, the increased time they spend away from home places increased strains and some increased risks both on the employee and their families. The travel security provider BizJet Security claims that 20 percent to 25 percent of expat assignments fail – and that security concerns are a major factor in those failures. For simplicity's sake, this whitepaper refers to all individuals away from their usual workplace as “travelers,” independent of the length of the trip.

How the U.K. Corporate Manslaughter and Corporate Homicide Act relates to corporate travel

This piece of legislation passed by the U.K. parliament has attracted intense attention (and several misunderstandings) within the corporate travel community not only in the U.K. itself, but also in Europe and North America. This is because it is expected to set a global trend for criminalizing failure to provide duty of care to employees.

The Act, which took effect on April 6, 2008, enables prosecution for a gross failing throughout an organization in the management of health and safety with fatal consequences. As a result, prosecutors no longer need to prove the culpability of any individual, but can instead prove corporate fault, although there must be substantial failure at the senior management level. There is no stated limit on potential fines.

With regard to how the Act relates to corporate travel, there are two common misconceptions:

a) Jurisdiction

The Act does not apply to which deaths occur outside the U.K., unless they are on British-registered ships or aircraft. However, it does apply to all deaths in the U.K., regardless of whether the organization is registered there or overseas.

b) Specification

The Act does not define what actions (or failures to take action) would be considered a gross failing. However, legal and security experts have suggested three broad areas organizations should consider in relation to business travel:

- **Risk assessment** – A risk assessment should be made for every journey to or within the U.K. For the overwhelming majority of business trips, this can be of a broadly generic type.
- **Communication** – Organizations must ensure travelers have understood and acknowledged the duty of care responsibilities of both the employer and the traveler.
- **Driving** – This is by far the greatest travel-related risk in the U.K. Examples of mitigating actions could include checking the documentation of drivers and their vehicles, or banning travelers from driving immediately after long-haul flights.

At time of writing, no prosecutions have been brought under the Act. The Ministry of Justice does not expect to see any until late 2009 at the earliest, owing to the lengthy nature of the police investigations that would be required. It has confirmed such investigations are under way. Legal experts have warned that even if organizations are not prosecuted successfully, they face serious disruption during the process of investigation.

BizJet Security claims that 20 percent to 25 percent of expat assignments fail – and that security concerns are a major factor in those failures



Section A

The connection between risk management, duty of care and corporate travel

How well do companies manage travel risk?

There is a paradox at the heart of this subject. Although, as described above, business travel is inherently risky, it is often overlooked or paid only scant attention. At a high level, it appears to receive less prominence than financial and strategic risks because travel-related risks are unlikely to put an organization out of business. At an operational level, travel is an area in which security departments tend to have limited expertise.

“My experience is that security managers only know about travel if they have talked to their travel managers,” says Andreas Krugmann, business travel industry international sales manager for the medical assurance and travel insurance group Mondial Assistance. As an example, Krugmann says corporate security trade fairs almost never feature travel-related exhibitors or seminar presenters. He adds: “Corporate risk management is very advanced but travel risk management is a child yet to mature.”

Challenges to successful travel risk management

Among the challenges inhibiting the development of travel risk management are the following:

Underestimation by the employer

A frequent comment made by travel security experts is that organizations do not take TRM seriously until a significant incident affects one of its travelers.

Travel also seems to be a blind spot when it comes to duty of care. Legal and security experts have observed that organizations devote far more attention to health and safety procedures in the permanent workplace than outside it, even though this is where potentially the greater risk lies. For example, there are an estimated 300 to 400 deaths per year in the permanent workplace in the U.K., but 800 to 1,200 deaths on the road involving people traveling in the course of their work. The Royal Society for the Prevention of Accidents says that driving more than 25,000 miles per year for work carries as much risk of a fatal accident as mining or quarrying.

Underestimation by the employee

Complacency and lack of awareness mean corporate travelers do not always appreciate the risks they face. While education is key, another solution can also be to make the regular breaching of travel risk policy a disciplinary issue.

Distorted perspective

Companies may appreciate the serious potential consequences of major incidents such as terrorism or kidnapping, but they also know the probability of such events is remote. With a focus on major incidents, organizations might overlook far more likely but less sensational and equally potentially serious risks such as road accidents or illness.

Fragmentation of responsibility

Initiating a TRM strategy involves numerous departments, including security, travel, medical, human resources and legal. If organizations do not deliberately create a structure or process to join up these departments, responsibility for TRM can slip between all of them. (This issue is covered in detail in Section B.)

Status of travel management

If the initiative for TRM originates with the travel manager, then the prospects for success depend on the travel manager being informed, proactive and well versed in what matters for the business. The standing of the travel manager within the organization is also important, because his or her ability to gain the attention of senior management is essential.

Staying up to date

Risk profiles can change overnight, either through external factors, such as security or political incidents, or internal factors, such as mergers and acquisitions and resulting changes in travel pattern. Organizations need to understand their exposure to new and changing risks.

Case study - Hewitt Associates

Serious about risk; serious about travel risk

Human resources outsourcing and consulting company Hewitt takes a highly coordinated approach toward risk management. In 2007, it appointed its first global chief security officer, whose responsibilities include physical and corporate security, safety, information security, data privacy, business continuity and supplier risk governance. "All too often, the left hand and right hand are not coordinated," says Hewitt director of corporate/physical security and safety Scott Maxson. "The appointment of a CSO has brought people out of their silos." The company has also appointed regional CSOs.

The raising of the profile of risk management in general has coincided fortuitously with Hewitt globalizing its travel program for the first time, including writing its first global travel policy. As Hewitt continues to expand its operations globally, the need for a well-planned travel risk management strategy has become more acute. As a result, security figures prominently in the global travel policy.

Although these structural changes have made developing a Travel Risk Management program easier, Hewitt Travel Director Kim Heche believes many organizations could create one even if they lack the strategic oversight of a CSO.

"It is not an absolute requirement," she says. "Instead, wanting to improve travel security has to be a priority and goal in each relevant area of the business. Scott and I made a deliberate effort to get together from the very start."

Shared management of travel risk

Hewitt regards Travel Risk Management as a shared responsibility between the travel and security departments, with a comfortable delineation of tasks. Travel is responsible for policy design, communications and compliance by third parties. Security is responsible for planning, situation monitoring, assessment and risk mitigation

Corporate risk management is very advanced but travel risk management is a child yet to mature



Section A

The connection between risk management, duty of care and corporate travel

Risk management maturity

In order to assess how well a company manages risks, a framework is required. A frequently used framework for assessment is a capability maturity model.

The Global Risk Management Committee of the U.S. National Business Travel Association (NBTA) has published a Travel Risk Management Maturity Model in association with the travel security intelligence and technology specialist iJET Intelligent Risk Systems. The model identifies five stages in the evolution of a TRM strategy:

Fig 4. Stages of evolution within Travel Risk Management strategy

Maturity level	Characteristics	Consequences and barriers
1. Reactive	Ad hoc. Few policies. Chaotic in the event of an emergency.	Organization at substantial risk. Could incur significant liability for not fulfilling duty of care.
2. Defined	Basic travel risk management policies defined and documented. Primary focus on incident response.	Many organizations at this level. Basic elements of good strategy but not consistent. Reactive rather than proactive. Failure to reach next level often because of reluctance to invest.
3. Proactive	Consistent execution of travel risk management processes.	The minimum to which organizations should aspire. Failure to reach next level is often because organization has no enterprise-wide risk management program.
4. Managed	Metrics collected and reviewed. Cross-organization support.	Formal program, consistently monitored with good training. Very few organizations at this level.
5. Optimized	Program integrated throughout organization.	Also includes process optimization program. World-class.

Source: NBTA, iJET, with some additional verbal observations in column 3 from Bruce McIndoe, president of iJET. A much fuller characterization of each maturity level can be found in the two organizations' jointly prepared white paper, Travel Risk Management Maturity Model (www.ijet.com/news/whitepapers).



A frequently used framework for assessment is a capability maturity model

Section B

How to create a travel risk management strategy

For the purposes of this white paper, Advito proposes the simplified model shown in Figure 2 (see Executive Summary, page 2) to help organizations start a TRM program:

1. Assigning management responsibility

Determining the personnel to contribute to building a TRM program is a complex and potentially discouraging task for two reasons:

- TRM involves numerous departments, including travel, security, HR, legal and medical.
- There are four different types of stakeholder involvement in the program:
 - The stakeholder(s) who initiate(s) the idea
 - The stakeholder(s) who provide(s) senior sponsorship to make it happen
 - The stakeholder(s) who is/are accountable for the program
 - The stakeholder(s) who manage(s) introduction and continuing management of the program

It is quite possible that each of these stakeholders will be different personnel within the organization, making the job of coordination difficult. Identifying who is the most appropriate stakeholder will vary according to the culture and structure of each organization, but below are some general guidelines.

Stakeholder 1 - Initiation

The initiative to create a TRM strategy could come in theory from any relevant department, or from senior management or the organization's risk management board, if there is one. In practice, however, travel security experts say it is usually the travel manager who is the first person in the organization to understand the need to manage travel risk. (The exception to this principle is if an organization is stirred into action by a serious incident affecting a traveling employee.)

Stakeholder 2 - Senior sponsorship

Who

"In my experience, without senior management support from the very top, the program will fail," says BizJet Security managing partner John Cosenza, a view shared by all other experts interviewed for this white paper.

"Support has to come from C-level, either the CEO or the CFO, who is usually the one responsible for risk management," says iJET president Bruce McIndoe. "Once they make it a priority, everyone else typically falls in line. Even if the strategy is not initiated at that level, it must be supported at that level."

In countries where non-executive directors have oversight of risk management, it is worth targeting them, too.

How

The wrong way to make the case to senior management is to over-sensationalize the issue. Instead, it is best to prepare a brief risk/reward document mapping out the potential risks and the liability – especially financial – that the organization would face if it did not take steps to manage and mitigate them.

Liability can range from the minor to the major. At the minor end would be loss of productivity caused by a traveler losing their personal baggage. In the middle would be the mugging of a traveler for their laptop computer, involving trauma and physical harm for the employee and the loss of commercially sensitive data. At the major end, empirical research has demonstrated a negative effect on a company's share price if more than two of its directors die in the same air accident.

It is also worth enlisting the support of key allies before presenting to the intended senior sponsor. For example, obtain support from the head of sales if most traveling personnel are in sales.

Stakeholder 3 - Accountability

This will usually be vested in the person who has responsibility for managing all risk within the organization, e.g., the CEO, CFO or managing director. Alternatively, it may be vested corporately in the risk management group or the departmental officer with responsibility for the most important travel-related risk. Example: If there is frequent travel to destinations with high disease risk and poor medical facilities, accountability may lie with the chief medical officer (if there is one).

Section B

How to create a travel risk management strategy

Stakeholder 4 – Management

It is essential to form a steering group with representatives from all relevant departments. It is also essential that a single person is given ownership of the TRM program to drive and coordinate the project. This person will need project and change management skills and the necessary time to undertake the work in addition to existing duties.

Once again, the departmental background of the manager may be determined by the overall strategic purpose of the program and/or department most relevant to the largest travel-related risk.

Outsourcing

It is almost inconceivable that a TRM program could be created and managed without outsourcing some tasks to third-party specialists. Advantages to bringing in third parties include:

Expertise

Security and travel security providers have developed models for creating and managing travel risk programs with knowledge of best-in-class set-ups.

Intelligence

Although government Web sites such as the U.S. State Department and the U.K. Foreign and Commonwealth Office are excellent sources of information, they are not entirely sufficient. A small number of security providers have developed information networks that pinpoint even more precisely the corporate market's needs and risk profile. Tailored with their ability to provide mitigation, it may be possible to visit destinations using a travel security provider's advice when a government Web site has advised against travel.

Technology

Some travel security provider and travel management companies have developed traveler tracking programs (see below under **4. Mitigate or Manage** for more details). They also provide data management services that can push relevant information to travelers.

Resource

There are some services from third-party providers that could conceivably be provided in-house, but for which the costs would most likely be higher. Example: a telephone answering service for an emergency assistance program.

Impartiality

The impartiality a third party can provide in reviewing an organization's travel risk profile should not be underestimated. Such a review is particularly useful for resolving inevitable conflicts of priorities between different stakeholders. A third party can lay out the options and mediate, pointing out the advantages and disadvantages of each option. In particular, they can point to industry best practice, a highly persuasive factor for those who deal with risk, such as legal counsel.

Travel management companies (TMCs)

TMCs play a crucial role in TRM. The bookings they make for corporate clients are the data source for traveler tracking programs. They also usually have responsibility for managing, communicating and enforcing travel policy, another fundamental aspect of travel risk management and mitigation (see below under **4. Mitigate or Manage** for more details). In addition, they maintain traveler profiles – invaluable for tracing and assisting travelers in an emergency.

Medical assistance

Organizations need to assess their insurance coverage and how they provide assistance. Specialized medical assistance companies can provide in-country medical care and/or repatriation in the event of illness or injury (see below under **4. Mitigate or Manage** for more details). Some organizations prefer to provide assistance independent of the incident being of medical and security nature and select an integrated provider.

Case study - The Capital Group of Companies

Managing travel risk through the travel department

The investment management group Capital Group deals explicitly with the concept of risk in its travel management program. It refers to duty of care in its travel guidelines and travel risk is considered by its senior management committee. In addition, group travel manager Stephanie Dillon liaises regularly with the risk management group, business continuity group and compensation and benefits group.

Dillon is from an oil company background and it was she who first drew the attention of senior management to the need for a Travel Risk Management program. She won

buy-in initially by convincing the risk management and business continuity groups of the importance of tracking travelers. Together with these two groups and human resources, Dillon has formed a travel risk sub-committee.

Dillon is the internal “owner” of Capital Group’s contract with International SOS, which provides traveler tracking and intelligence services as well as security expertise. Capital Group does not have a stand-alone in-house security department. Dillon is the first point of contact within Capital Group in the event of traveler emergencies.

Case study - ING

Managing travel risk through the security department

Risk management is a major strategic priority for the financial services company ING. One of the company’s board members includes risk in his portfolio of responsibilities. The company regards itself as an innovator in the importance it attaches to the subject.

Travel is increasingly regarded as a crucial area of risk management within ING. The welfare of the traveler – including health and safety as well as security – is also now understood as a business continuity issue.

In a reflection of ING’s corporate structure, overall responsibility for Travel Risk Management lies within

the security department. The company has a corporate department, based at global headquarters in Amsterdam, and six business lines. Security is part of the corporate department, giving it global reach and the ability to manage travel risk consistently across the world. In contrast, travel is not yet managed globally. ING uses numerous TMCs.

The situation is changing. ING intends to consolidate to a handful of TMCs worldwide. It has also launched an internal project to coordinate Travel Risk Management across other relevant corporate functions, including human resources and health and safety.

Case Study – DuPont

Managing security globally in a concerted manner

Safety and security are key internal focal points for DuPont. Country, regional and global security personnel are responsible for the security of DuPont employees around the world. Although final responsibility for Travel Risk Management falls under the global security team, this group works in concert with the travel management, medical, crisis and information security teams.

Travel is managed globally, and security reporting is provided by DuPont’s TMC. Reports are available to DuPont 24x7 in a “follow-the-sun” strategy in which each region is responsible, during their hours of operation, for notifying DuPont of any type of event where employees may be at risk. The travel

management team, in conjunction with the local or regional security team, works to establish the whereabouts of every traveler who may be in an affected area or situation, sharing and transferring information to an internal tracking system until each employee is located.

Crisis teams support the safety and security of employees at all company locations, with particular emphasis on plant locations. A response team works intra-organizationally to support locations during storms or other outages. The team has established processes and procedures for the most common events, including natural disasters; such plans are managed closely and updated annually.

Section B

How to create a travel risk management strategy

2. Determine risk types

To understand the scope of your organization’s risk exposure, we suggest creating a matrix similar to Figure 1 on page 2, specifying travel-related risk types and sub-types.

An alternative model for developing a risk plan would be to divide risks into three chronological groups: pre-trip, on-trip and post-trip.

It should be noted that not all risks are equal, either in their probability or in the severity of their consequences. In the context of travel, risk to personnel is more important than anything else. “An organization can recover from legal and financial travel-related risk but if a person is killed or disabled, it is much more traumatic for the work force and much harder to recover,” says J. Randy Ryan, chairman of the transportation council of ASIS International, a worldwide association for security professionals.

It may well be worth attaching a weighting to more important risk types as seen by the company so that initiating a program to assess and mitigate them is given priority and supported by all stakeholders.

3. Assess risk exposure

There are two types of assessment of travel risk exposure:

Strategic – an assessment of the effectiveness of the entire TRM program

Tactical – an assessment of the organization’s exposure to specific threats

Strategic

The NBTA/ijET Risk Maturity Management Model mentioned above provides a framework for assessing the condition of an organization’s TRM program. It breaks down a TRM program into 10 Key Process Areas (KPAs) and then defines how well an organization at each of the five previously described levels of maturity would perform in each KPA.

For example, one of the KPAs is risk assessment. An organization at Level 1 (Reactive) has “no established practice or standards.” For an organization at Level 3 (Proactive), “risk assessment is consistently applied to each trip based on defined risk criteria”. Appendix A of this white paper carries the NBTA/ijET KPA Rating Matrix in full.

NBTA and ijET suggest stakeholders individually make a quick, rough assessment of which stage of maturity they believe their organization has reached for each KPA, along these lines:

Fig 5. Sample calculation of risk assessment maturity

Key Process Area	Level 1	Level 2	Level 3	Level 4	Level 5
Policy / Procedure			x		
Training		x			
Risk Assessment		x			
Risk Disclosure			x		
Risk Mitigation		x			
Risk Monitoring			x		
Response					x
Notification		x			
Data Management			x		
Communication					x
Level		x			
Travel Risk Management₃ Rating: Level 2 – Plus 6					

Source: NBTA/ijET

After that, the assessment can be re-visited in more detail, paying particular attention to where different stakeholders gave different KPA ratings.

Tactical

A quick assessment of exposure to specific threats can be made by developing the risk type matrix shown in Figure 1, listing the organization’s likely exposure to each risk type based on its travel profile. An example of this would be Figure 6.

Fig 6. Sample assessment of specific exposure

This matrix is for illustrative purposes only and is no way intended to be a complete assessment of risk exposure.

Risk type	Risk sub-type	Exposure
Risk to personnel	Security (crime/civil unrest)	Civil war – Democratic Republic of Congo
	Security (terrorism)	Bomb attacks – Jakarta
	Safety	Driving after long-haul flight
	Health (illness)	HIV – sub-Saharan Africa
	Health (stress)	Fatigue through over-travel
Risk to reputation	Failure in duty of care to employees	Contracting disease owing to lack of inoculation
	Carbon footprint	Criticism from ethical investors, analysts and pressure groups
	Misuse of travel expenses	Criticism from auditors
	Unethical conduct by employees	“Honey traps,” e.g., in former Soviet Union
Risk to data/equipment	Data carried by travelers	Laptop theft
	Data collected about employee travel	PNR and APIS data collection – U.S.
	Baggage, equipment and personal items	Passport theft
Legal risk	Duty of care/health & safety legislation	Corporate Manslaughter & Corporate Homicide Act – U.K.
	Data protection regulations	Forwarding of traveler profiles to third-party traveler tracking tool providers
	Failure to comply with tax laws	Incorrect reclamation of VAT incurred overseas
	Illegal activity by travelers	Attempts to corrupt government officials
Financial risk	Financial penalties of exposure to legal risk	Unlimited fines under Corporate Manslaughter & Corporate Homicide Act –U.K.
	Misuse of travel expenses	Upgrading to suite at hotel check-in
Risk to productivity/trip effectiveness	Baggage, equipment and personal items	Baggage lost by airline leads to missing important meeting
	Inadequate technology or support for travelers	Standard-issue mobile phone does not function – Japan
	Failure to meet immigration requirements	Failure to obtain electronic travel authorization – Australia and U.S.

The opposite table is necessarily a simplification. Risk exposure needs to be assessed in terms of the severity of the threat balanced against the organization's exposure to that threat. Data is needed to provide a context in which to make such an assessment. Relevant factors include:

- The countries to which personnel travel
- Whether they stay in one place or move to other locations
- Standard of travel (e.g., staying in five-star hotels or rudimentary field accommodation)
- Transient travel or long-term expat assignment
- What travelers take with them (e.g., laptops)
- Vulnerability of personnel (e.g., experience, gender)

An organization must also consider its appetite for risk. Almost any travel-related threat can be mitigated but is the organization comfortable with the level of risk that remains after mitigation? And is it worth the expense? As an extreme example, is it prepared to send personnel to certain parts of Mexico or Colombia, even after providing them with training about kidnapping?

Section B

How to create a travel risk management strategy

4. Mitigate or Manage

The four Ts

Risk managers refer to the four Ts, which are the four basic ways risk exposure can be mitigated or managed:

Treat – This does not necessarily mean eliminating the risk but containing it to an acceptable level via internal controls.

Transfer – Persuading or paying a third party to take the risk in another way, such as insurance.

Terminate – The risk is only treatable, or containable to acceptable levels, by terminating or aborting the activity.

Tolerate – Ability to mitigate the risk actively is limited, or the cost of taking action is disproportionate to the potential benefit gained. As a result, the response is simply to tolerate it.

Examples of travel risk mitigation

There are numerous procedures and investments through which organizations mitigate travel risk. What follows is a basic guide rather than a complete list, but it provides a useful snapshot of the main issues to be considered.

Process

Recruitment

There is a case for introducing travel risk management as early as the recruitment phase. Candidates for positions likely to involve frequent travel or travel to higher-risk destinations can be assessed for their suitability in terms of both their physical health and temperament. Show them the organization's travel risk policy (see below) so they know what will be expected of them.

Booking

Organizations at the forefront of risk management practice have built automated processes in which the destination for every reservation made through their designated TMC is classified according to risk level. Each booking – both directly with the agent and/or online – will then trigger a different response according to the risk rating, as shown in figure 7.

Fig 7. Sample destination-specific mitigation processes at booking

This matrix is for illustrative purposes only and is no way intended to be a complete assessment of risk exposure.

Country	Risk rating	Mitigation
Belgium	Low	None
Russia	Medium	Permission required from line manager Written destination briefing Inoculations check Airport meet and greet
Saudi Arabia	High	Permission required from chief executive One-to-one training Inoculations check Airport meet and greet Liaison with company representative at destination Registration with embassy on arrival
Democratic Republic of Congo	Extreme	Permission required from chief executive Comprehensive individually created plan for close health, safety and security

The risk must be assessed not only according to the country the traveler is visiting but also where specifically in the country they are visiting, with a clear matrix of consequences to follow. This could be as simple as a three-way choice between travel refused, approval required or briefing required.

It is also important to construct the process so that tickets are not released to the traveler until the trip has been through the specified approval and mitigation procedure. This requires clear instruction to the TMC. For instance, if employees are not allowed to travel to Somalia, the TMC must be instructed to block bookings to that country.

Other instructions that can be built into the booking process include blocking reservations on carriers blacklisted for a poor safety record and setting a limit for the number of employees or directors allowed on the same flight.

Traveler tracking

Traveler tracking systems became more widely available in the aftermath of 9/11 and have proved extremely effective in pinpointing the whereabouts of travelers following terrorist incidents, natural disasters, air crashes and other emergencies.

“We are very much in favor of them, even for medium-size companies,” says John Cosenza of BizJet Security. “It is the only way to respond quickly to an incident when the CEO calls to ask if any personnel are involved. If a CFO asks how much one costs, tell them to look at the overall travel budget. The cost is tiny in comparison – thousands, not millions, of dollars.”

Tracking systems take a feed of all trip bookings from the TMC. Provided the bookings in question are made through the designated channels, travel managers, security and HR managers can then interrogate the systems to see at-a-glance information such as:

- Who is staying in a particular city
- Who is staying at a particular hotel
- Who is on a specific flight
- Who is booked to travel to a destination or has returned from it within recent weeks

Some traveler tracking systems have been developed by travel security providers and others by TMCs. However, regardless of origin, intelligence and/or security providers and TMCs are interdependent. The TMC-built systems rely on destination intelligence from a third-party security source, whereas those built by security providers require information from the TMC about the organization’s travel bookings.

Whether it is better to choose a TMC-built or security provider-built tracking system depends on the organization’s security requirements, program consolidation status and budget. A TMC-built system puts the client closer to the travel data, whereas the security provider-built system is closer to the intelligence and to on-the-ground incident support services.

Regardless of the technology solution chosen, the most successful programs are those that have a strong mandate for using their designated booking channel (e.g., the travel management company and/or online booking tool of choice) for all bookings and changes to original bookings for all travel components, including air, hotel and car. In turn, the designated TMC needs to have strong operational and workflow processes to ensure that all data migrates through to the security tool.

A number of organizations are also investigating how best to complement traveler tracking with alternative data sources, most notably through corporate card expenditure.

Away from these deliberately developed systems, there are other, more rudimentary, forms of traveler tracking that may also have a role to play. These include issuing travelers with global positioning system-enabled mobile telephones or even instructing travelers to make regular calls to keep the company apprised of their location.

Section B

How to create a travel risk management strategy

Case study - PricewaterhouseCoopers UK Risk management at point of booking

Risk management for travelers from PwC UK kicks in at the moment they book a trip. Thanks to well-designed automation, the choice of destination by the traveler triggers a series of mitigating actions including:

- A trip approval process
- Distribution of security information to the traveler
- Initiation of additional precautions

PwC UK believes that initiating risk management at point of booking has distinct advantages. The first is that it fulfils duty of care obligations by ensuring travelers and those who manage them are aware of the risks and how they are mitigated.

“We realized that security considerations needed flagging at the point of booking rather than putting information on the portal and telling travelers they should read it,” says head of U.K. security Richard Stanley.

The second advantage is that automating the process is

not only effective but efficient. The PwC security team has five personnel, of whom one spends 20 per cent of his time managing travel issues. “It is the system that does the work, not us,” says Stanley.

How the process works

When a traveler books a trip through PwC UK’s appointed TMC or online booking tool, their chosen destination is risk-graded as either normal, medium, high or extreme. The gradings are based on intelligence from travel security providers Control Risks and International SOS, and the U.K.’s Foreign & Commonwealth Office.

If the booking is to a normal destination, it is ticketed as usual. If it is to any other grade of destination, then it is held without being ticketed while an alert is sent to the security department. In turn, the security department contacts the traveler to advise them of the risk level and provide them with a risk assessment. In addition, the following steps are taken, according to the risk type of the destination:

Risk Level	Approval Source	Other mitigating actions
Medium	Business unit leader (usually the line manager)	Written security briefings: a) guide to country’s political, travel and security risks; b) specific briefing on location being visited
High	Head of one of PwC U.K.’s three lines of business	More detailed preparation, e.g., face-to-face briefing
Extreme	Board-level	Intensive planning, e.g., hiring of bodyguards

Most travel security professionals recommend the creation of a travel risk policy separate and distinct from the main corporate travel policy



Traveler profiles

Traveler tracking systems are of little use if travelers cannot be contacted to check that they are safe and to offer them assistance. It is therefore essential to keep the employee profiles updated in a system readily accessible by those who might need to coordinate the communication. In those profiles, emergency contact numbers for both the employee and their families should be held. There should be a mechanism that regularly pushes profiles to travelers for updating.

For higher-risk, if not all, destinations, travelers should be required to provide itineraries for their entire trip, including details of whom they are meeting and where, and how they will travel to the meeting if it is not at their place of residence.

Process/Information

Policy

Clearly, the processes above will not succeed unless they are linked to travel policy. In particular, not only the flight but also accommodation and all other travel components must be booked through the approved TMC or online booking tool. If this compliance is not achieved, processes such as traveler tracking will be redundant. However, mandating cannot be applied in a vacuum. Even the strictest mandate will not succeed if the standard of the TMC or booking tool is not high. Employees will find other ways to book their travel if they are frustrated, so a well-organized travel program is an essential precursor to a good TRM program.

Most travel security professionals recommend the creation of a travel risk policy separate and distinct from the main corporate travel policy. This separation helps ensure that the travel risk has maximum impact on employee thinking and to emphasize that the organization takes its duty of care responsibilities very seriously. If it is split from the general travel policy, the latter document should refer to the separate travel risk policy and give a high-level summary of its main points.

Employees should give written confirmation that they have read and understood the travel risk policy, which is normally in two parts:

- What the organization undertakes to do to mitigate or manage travel risk
- What the traveler is required to do to mitigate risk

Once again, the traveler should provide written agreement to meet the specified requirements.

Examples include:

- Behavior
- Dress
- Commitment to provide itinerary details
- Contacting the embassy on arrival
- Not changing flights at the airport (something that would not be picked up by a traveler tracking tool)

The travel risk policy also specifies who has authority to approve a trip.

Case study – Hewitt Associates

Cracking down on out-of-policy hotel bookings

Hewitt has high levels of compliance for travelers booking flights through the official online and travel management company channels. However, as for almost all companies, channel compliance for hotel reservations is less satisfactory. The company is anxious to improve this situation for security tracking as well as procurement reasons, and is taking the following remedial measures to

address the issue:

- Urging travelers to book their hotel at the same time they book their flight
- Offering to book hotels chosen by the traveler's client at the client's rate (a frequent source of non-compliance)
- Extensive communication, including posting messages through the online booking tool

Section B

How to create a travel risk management strategy

Case study – PricewaterhouseCoopers UK Mandating booking channels to meet duty of care obligations

PwC UK has a highly autonomous internal culture, as a result of which it is not generally considered acceptable to mandate behavior. However, the firm has made an exception by tightening travel policy to specify that bookings must be made through the approved TMC or self-booking tool. This is to ensure all bookings can be

graded and mitigated according to the risk classification of the destination (see above) and so that travelers can be tracked in an emergency. As a result of the mandate, bookings through approved channels have risen from 88 percent to 96 percent.

Action plan

Provide guidelines for who needs to respond to incidents affecting travelers. This includes:

- Travelers knowing whom they need to contact. Is it someone within the organization, and if so, whom? The travel manager? The security department? Or is it a third party, such as a contracted emergency assistance organization? Is it both? Whatever the procedure, it should be printed on a credit card-sized document and distributed to all travelers.
- Other personnel knowing whom to contact in turn if they are contacted by a traveler. Once again, they need to know which personnel to alert internally. There should also be a procedure for liaising with the traveler's family.

Information

Security tips

Create and distribute a list of general safety tips, plus an extra list for travel to higher-risk destinations. See Appendix B for examples.

Destination information

It is arguably worth providing travelers with information about all destinations – certainly for any destination above the lowest risk ratings, whether for security, safety, health or even cultural reasons. Among the types of information that would be of use are:

- Required mitigating actions
- Specific security tips – e.g., no-go areas within the city, impending flashpoints for insecurity (such as elections)

- Appropriate cultural behavior
- Entry and exit requirements
- Health issues – required inoculations, availability of health facilities and medicines, proscribed medicines, etc.
- Payment methods
- Telecommunications specifications
- Internal travel by road, rail and air
- Emergency procedures and contact details

It is much more effective – and arguably an obligatory duty of care – to push information to travelers than to rely on them searching for it on the corporate intranet. However, it is worth posting on the intranet too, so travelers can understand the risks associated with a destination at the beginning of their trip planning process. Also worth considering is pushing relevant updated information to employees who visit that destination regularly, even if they have no trips pending. Either way, getting the balance right between providing enough information and avoiding information overload is crucial.

As discussed earlier, a small number of travel security providers source and write the types of destination information described above. They have also developed processes used in conjunction with TMCs to push the relevant information to the relevant travelers. These are highly recommended. Enquire whether your TMC has a commercial relationship with any such providers. It may prove cheaper and more seamless to source through the TMC than dealing with the provider directly.

Case study – Hewitt

Sourcing “Hewitt-ized intelligence”

Hewitt obtains most of its travel intelligence from the travel security provider iJET Intelligent Risk Systems. Unusually, however, iJET provides a dedicated analyst who works solely on the Hewitt account, filtering information and releasing assessments specific to Hewitt’s locations and spheres of operation. “It ensures we get what we call ‘Hewitt-ized intelligence,’” says Hewitt director of corporate/physical security and safety Scott Maxson. “iJET provides very good off-the-shelf intelligence but what concerned us was whether it was relevant to us. This takes

it to the next level by avoiding information overload.”

The dedicated Hewitt analyst at iJET has been immersed in the client’s culture and briefed thoroughly on the location of its offices, even to the extent of visiting some of them. Hewitt does not consider the investment in a dedicated analyst expensive. “We see it as saving a lot of money by giving us good knowledge and anticipation of events without having to put someone on our payroll,” says Maxson.

Planning

Crisis management

Planning should be developed in conjunction with the internal security department and/or third-party advisers. Specific plans, such as evacuation plans, are clearly necessary for high-risk destinations, but general contingency planning is also important, e.g., buying policies with air charter brokers that ensure priority allocation of private aircraft in the event of scheduled aircraft services being disrupted.

On a smaller scale, but similarly important, are event-specific plans. Be it the annual general meeting, quarterly board meeting or any other events where complete units or senior management come together, it is important to develop plans that prepare for crisis situations.

Another important aspect of crisis management planning is to have clear delineation of responsibilities. Appendix C provides sample flow charts showing which personnel are involved in a crisis response and what their duties are.

Risk transfer

Insurance

Travel insurance is often purchased without the attention it merits. It is dangerous to buy on price alone. Whoever is responsible for buying insurance needs to be aware of the TRM program. In particular, they should learn from the travel manager which destinations the organization’s travelers are likely to visit, and especially which higher-risk areas they are

likely to visit.

It is strongly advised to avoid policies that:

- Exclude acts of terrorism
- Exclude specified destinations
- Limit cover

In the case of terrorism exclusion, it may be possible to negotiate the removal of this clause for a small fee. Another pitfall to watch out for is whether the policy includes third-party nationals.

The legal department should always examine any insurance contract.

Medical assistance

Medical assistance companies can help in incidents by providing swift and expert treatment, either by treating the patient on-site, finding a high-quality hospital or repatriating them by air. Apart from the fact that it is impossible for any organization to have the requisite coverage and expertise itself, the cost of treatment without insurance can easily exceed US\$1 million per patient.

Mitigate your risk exposure

Using the various types of mitigation and the four Ts explored above, it is now possible to add a new column to the risk matrix shown in part 3. The new column specifies the mitigation that can be made for each identified risk exposure. Here, once again, is a simplified example:

Section B

How to create a travel risk management strategy

Fig 8. Sample assessment of specific exposure with proposed mitigation

This matrix is for illustrative purposes only and is no way intended to be a complete assessment of risk exposure.

Risk sub-type	Exposure	Mitigation
Security (crime/civil unrest)	Civil war – Democratic Republic of Congo	Terminate – Ban all travel to destination
Security (terrorism)	Bomb attacks – Jakarta	Treat – Introduce traveler tracking
Safety	Driving after long-haul flight	Treat – State in policy that travelers must use taxi or drive the next day
Health (illness)	HIV – sub-Saharan Africa	Transfer – Subscribe to medical assistance service Treat – Provide travelers with syringes
Health (stress)	Fatigue through over-travel	Treat – Introduce health checks for frequent travelers
Failure in duty of care to employees	Contracting disease owing to lack of inoculation	Treat – Provide free inoculation service; require travelers to be inoculated before travel
Carbon footprint	Criticism from ethical investors, analysts and pressure groups	Treat – Introduce video-conferencing; mandate rail where appropriate; etc.
Misuse of travel expenses	Criticism from auditors	Treat – Introduce expense management tool
Unethical conduct by employees	“Honey traps” – former Soviet Union	Treat – Warn travelers of dangers in destination information
Data carried by travelers	Laptop theft	Treat – Set enterprise-wide standards for data encryption
Data collected about employee travel	PNR and APIS data collection – U.S.	Treat – Inform travelers to U.S. how their personal data will be treated
Baggage, equipment and personal items	Passport theft	Transfer – Obtain travel insurance including emergency assistance
Duty of care/health & safety legislation	Corporate Manslaughter & Corporate Homicide Act – U.K.	Treat – Introduce trip risk assessments
Data protection regulations	Forwarding of traveler profiles to third-party traveler tracking tool providers	Treat – Ensure tool providers comply with EU regulations, U.S. Safe Harbor, etc.
Failure to comply with tax laws	Incorrect reclaim of VAT incurred overseas	Treat – Subscribe to VAT reclaim service
Illegal activity by travelers	Attempts to corrupt government officials	Treat – Prohibit corrupt behavior in employees’ terms and conditions
Financial penalties of exposure to legal risk	Unlimited fines under Corporate Manslaughter & Corporate Homicide Act –U.K.	Treat – Introduce trip risk assessments
Misuse of travel expenses	Upgrading to suite at hotel check-in	Treat – Obtain hotel e-folio data; prohibit upgrades in policy
Baggage, equipment and personal items	Baggage lost by airline leads to missing important meeting	Treat – Specify in policy how much travelers can spend to replace lost baggage
Inadequate technology or support for travelers	Standard-issue mobile phone does not function – Japan	Tolerate – (Limited travel to Japan; not important)
Failure to meet immigration requirements	Failure to obtain electronic travel authorization - Australia	Treat – Instruct TMC not to book travel until traveler has obtained authorization

Case study – The Capital Group of Companies

Working with the travel management company and third-party security provider

Capital Group mitigates much of its travel-related risk through its travel management company, BCD Travel, and by engaging the services of security and medical assistance provider International SOS. All bookings through BCD Travel are queued to International SOS, which sorts them into low-, medium-, high- and extreme-risk tiers according to the destinations that will be visited on the trip. Bookings to high- or extreme- risk destinations automatically trigger the sending of an advisory to the traveler covering medical, safety, security and other issues.

As an additional security measure, every week BCD Travel provides Capital Group with a full list of which personnel are booked to travel to which destinations in the fortnight ahead. The travel manager shares this list with senior management and advises them to check their travelers are

insured, inoculated and aware of potential risks relating to the destinations they are visiting. If extra measures are required for higher-risk destinations, such as the hiring of drivers or close protection, this is obtained through the overseas security provider Control Risks Group.

International SOS also provides a traveler tracking system that allows the Capital Group travel manager to pinpoint the whereabouts of personnel according to the bookings they have made. In addition, International SOS has a contract to provide evacuation and medical assistance to Capital Group travelers.

Another risk-related service provided by BCD Travel is that it informs the Capital Group travel manager if more than five personnel are booked to travel on the same flight.

5. Communicate

Proactive

As is the case with all issues directly affecting personnel, communication is an essential yet frequently overlooked element of a TRM program. “I know of companies with really good insurance cover but no one knows about it. For example, they are not given a wallet card detailing emergency assistance contacts,” says Andreas Krugmann of Mondial Assistance.

However, getting proactive communication right is a difficult balance. Some security professionals urge compelling employees to acknowledge they have read security communications. While that makes sense in terms of meeting duty of care obligations, it places an onus

on the sender to exercise discretion by only distributing material that is relevant and ensuring it is clearly and concisely written. If not, communication can become counter-productive, as when recipients acknowledge receipt reflexively instead of genuinely reading and understanding the documents.

It is recommended that travel risk be covered during employee induction. Another important option to consider is whether to produce a branded security program for your organization. This becomes especially relevant when using travel advisory and other services from third-party providers. Internal branding, paired with an end-to-end workflow and clear responsibilities, allows for a seamless change of providers without travelers noticing.

Section B

How to create a travel risk management strategy

Case study – ING Keeping travelers informed

ING's security department prepares its own assessments and risk ratings of destinations and communicates these through the company's business travel Web site, where they are available for all employees to read. The assessments provide a briefing on both political and security risks and are based on information from numerous sources, including:

- Specialist travel security providers
- Media organizations
- State foreign affairs departments
- ING security officers
- Security officers at other companies

Changes are made to the assessments at short notice. In the case of the Mumbai terror attacks of November 2008, the advice for travel to India was revised within two hours of the first news emerging.

In addition to being posted on the Web site, changes in assessments or advice are communicated proactively to executives who travel regularly, as well as to local business travel and security personnel

Reactive

Unfortunately, in spite of the best efforts to instill awareness in travelers, the best opportunities for achieving change often follow, rather than precede, incidents. If, for example, a laptop is stolen, it is well worth circulating information about laptop security, including how to avoid thefts, the need to encrypt all data and how to avoid data being overseen or intercepted.

Feedback loop

TRM programs rely on intelligence. While third-party providers play an important role in providing that intelligence, so do your own corporate travelers. They experience the selected suppliers first hand and can provide valuable feedback around a hotel in the corporate hotel program that does not live up to its security standard, which restaurants are close by, where to find reliable ground transportation, etc.

Providing a platform for travelers to share experiences and tips can provide the missing pieces of information in a language the traveler understands. This platform does not require a fancy social media solution; it can be as easy as conducting a debriefing session with expatriates returning home or soliciting feedback via a survey to returning business travelers.

6. Audit

It is a constant peril of corporate initiatives that, once implemented, they lose focus and momentum and eventually collapse from disuse. A TRM program is no exception, and in this case, neglect is particularly dangerous because travel-related risks are constantly changing.

However, it is precisely because risks are so numerous and variable that organizations are unlikely to become complacent. At a tactical level, there will always be a steady stream of advisories and incidents reported in the news to maintain traveler awareness.

It is also important to audit at a strategic level to test the robustness and relevance of the program. Techniques for maintaining continuity may include the following:

Travel Risk Management group

Although, as has been discussed, creating a TRM program is complicated by the need to achieve inter-departmental collaboration, this becomes a strength once the program is up and running, as necessary connections to departments including travel, security, HR, risk and legal are already established. Representatives from each can be drawn into a TRM group that meets regularly.

Providing a platform for travelers to share experiences and tips can provide missing pieces of information in a language the traveler understands



Risk maturity model

Measure progress in building the TRM program and benchmark against other similarly sized organizations at regular intervals, e.g., by using the NBTA/ijET Risk Maturity Management Model.

Plan ahead

Input is needed from senior management on destinations likely to be visited for the first time or more heavily than in the past. This input should be incorporated into the assessment and mitigation process.

Tap traveler expertise

“Frequent travelers are often the best corporate security managers,” says Andreas Krugmann of Mondial Assistance. Create a facility on the corporate intranet for travelers to report incidents, such as experiences of poor medical facilities or restaurants where suspected card fraud took

place. This feedback serves a dual purpose: the information can be forwarded to other travelers and it helps build up a risk and incident picture for security and travel managers.

Learn from experience

Incidents will inevitably happen. When they do, use the occasion not only as a good opportunity to remind travelers of relevant policy and procedures but also the chance to review those policies and procedures to see if the organization could have done better.

Monitor compliance

Keep a watchful eye on policy compliance, especially with booking travel through approved channels (TMC and booking tool). If compliance levels are low, it may be necessary to get tougher with persistent offenders, but it should also be a warning signal that elements of policy are genuinely unreasonable or unworkable for travelers.

Case study – Hewitt Associates

Auditing for blind spots

Following two major emergencies in 2008 – Hurricane Ike in Texas and the Mumbai terror attacks – Hewitt carried out audits to see how comprehensively its traveler tracking system identified all employees in the affected locations. It conducted the audit by comparing the information provided by ijET, supplier of its traveler tracking system, with bookings made through its TMC.

In both cases, Hewitt found very few gaps in coverage. Further investigation determined that the oversights which had been exposed could be attributed to internal causes, usually as a result of booking amendments by employees on long-term travel assignments not being recorded. The company is taking steps to eliminate these oversights.

Appendix A

KPA Rating Matrix

Key Process Area	Level 1 Reactive	Level 2 Defined	Level 3 Proactive	Level 4 Managed	Level 5 Optimized
Policy / Procedures (PP)	No defined Travel Risk Management policies or procedures to maintain them	Defined Travel Risk Management policies, ad hoc implementation	Defined Travel Risk Management policies and procedures; implementation across the organization as part of work process	Policies and procedures embraced throughout organization; fully integrated into corporate processes	Policy and procedure improvement procedures; feedback and lessons learned regularly examined and used to improve documented policies and procedures
Training (TR)	No or little training around Travel Risk Management	Basic traveler training defined and provided for high risk travel at minimum	Traveler and Travel Advisor training defined, documented and consistently delivered; integrated into the travel business process	Training requirement integrated into travel authorization; training history maintained; exercises and drills conducted	The training program includes an improvement process; metrics drive training effectiveness; training provided based on risk, location and/or special situation
Risk Assessment (RA)	No established practice or standards	Basic standard and process defined to evaluate risk of a trip	Risk assessment is consistently applied to each trip based on defined risk criteria	Management is actively engaged in reviewing risk assessments; risk assessment tied into travel policy	Improvement process in place to review and enhance the risk assessment process; metrics are captured to support decision-making
Risk Disclosure (RD)	No established practice or standards	Basic, documented process is defined to provide risk disclosure to the traveler before the trip	Risk disclosure information is provided prior to each trip	Risk disclosure information is continually updated throughout	Process improvement in place to measure and enhance the risk disclosure process; lessons learned are examined and used
Risk Mitigation (RM)	No established practice or standards	Basic, documented processes to mitigate certain risks	Active involvement by management for risk mitigation; high-risk trips have formal review and plan	Management is actively engaged in organization-wide risk mitigation; process is consistently applied to each trip exceeding a risk threshold	A process is in place to continuously improve risk mitigation strategies and implementation; lessons learned are captured and incorporated into documented procedures

Source: NBTA/ijET

Key Process Area	Level 1 Reactive	Level 2 Defined	Level 3 Proactive	Level 4 Managed	Level 5 Optimized
Risk Monitoring (RMON)	Ad hoc awareness of threats or hazards	Basic process is established and documented to monitor potential threats or hazards	All hazard monitoring program continuously operating 24x7; monitoring integrated into Risk Disclosure process	Risk monitoring program uses itinerary data to focus effort ; Monitoring integrated Risk Disclosure and Notification process	Process improvement procedures utilized to ensure continuous improvement of the monitoring process with emphasis on predictive threat identification; metrics and lessons learned captured and used to enhance process
Response (RP)	Response program is ad hoc	Basic response program is defined and documented; gaps identified but may not be addressed	Documented response program is consistently applied; cross functional integration and communication	Central authority for the response program established; integrated into the organization's emergency response program; metrics collected and reviewed; drills and exercises included in Training program	A process is in place to continuously improve the response program; metrics and lessons learned drive response speed and effectiveness
Notification (NT)	No notification procedures or tools	Basic process defined and documented to provide risk notification	Consistent processes are utilized to provide risk notifications; notifications sent to all appropriate recipients	Notification process collects and retains message history and metrics; notification process integrated into overall organization crisis management program	Metrics and lessons learned are examined and used to improve the notification process
Data Management (DM)	No data systems to support Travel Risk Management	Basic data systems to support traveler tracking	Integrated data management to support risk assessment, risk disclosure , tracking notifications and communications; trip data archived	Continuously updated and integrated data management in support of the Travel Risk Management program; quality review process implemented; metrics collected and monitored	Improvement process in place to continuously improve the scope and quality of the data; metrics and lessons learned are used to improve the data management program
Communication (CD)	No or ad hoc communication with stakeholders	Basic and documented program around risk communications	Communication integrated into the travel business process; consistent processes used to distribute information	Organizational management engaged in Travel Risk Management communications program; multi-level and multi-modal communications program	Improvement process in place to capture and apply feedback and lessons learned; metrics are captured to support the improvement program

Source: NBTA/IJET

Appendix B

Sample travel security tips

Disclaimer: These tips are based on real life examples tailored for one organization. The list is not exhaustive and requires vetting before using for your own program.

General tips

You should travel as anonymously as possible.

Travel in casual dress. Refrain from wearing expensive jewelry and watches or carrying expensive luggage. Try not to look “valuable.”

Do not permit yourself to be sought in the airport using your name.

Do not let those meeting you use a card bearing the company name or logo.

You should choose who is to carry your luggage and which taxi you are to use; do not let others choose for you.

Take the next taxi in line.

Try to choose a hotel room located between the third and the tenth floor.

Secure your hotel room door using all available locks.

If there is an unannounced caller at the door, verify with the hotel that they have sent a hotel employee before answering the door.

Always check to find the nearest exit in case of fire or other emergency.

Always use hotel safes to secure valuables (jewelry, watches, tickets, and passports).

Always carry a copy of your passport (and visa, if required) in your luggage and leave a copy at home.

Once checked into the hotel, lock your passport in your room safe and carry the passport copy with you.

Do not carry more cash or credit cards than are necessary at the moment.

Do not respond to loudspeaker calls in the lobby or dining room of the hotel unless you are expecting a call or a caller.

Valuables and negotiable documents (traveler’s checks) should be kept on the person or in tote bags but never in checked luggage.

Travel to hot spots

Take off all company tags, logos, etc., from luggage and clothes.

Make reservations through your global travel agency. They have been instructed to remove the company name from all tickets and itineraries.

Use a charge card that is not branded with the company name or use a personal credit card.

When registering in a hotel, use only your name, not the company's name.

Do not identify your company to immigration or customs officials.

Note on immigration forms that the purpose of your visit is to attend a conference – not specified.

Inform only your family and one or two colleagues of the details of your travel.

In politically unstable countries, you should register your name and passport number with your Embassy. Passports should be kept secure at all times.

Avoid leaving the hotel at the same time and following the same route every day.

Appendix

Sample flow charts of crisis management responsibilities

Stage	Team	Actions & Decisions						
Initial Notification Stage	<div style="border: 1px solid black; padding: 5px;"> <p>Designated Global Associates</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Travel Manager</td> <td style="width: 50%; padding: 5px;">Travel Specialist</td> </tr> <tr> <td style="width: 50%; padding: 5px;">Others</td> <td style="width: 50%; padding: 5px;"></td> </tr> </table> </div>	Travel Manager	Travel Specialist	Others		<ul style="list-style-type: none"> • Either learns of incident • Lead determines whether any travelers are affected (default lead determined by time of incident) 		
Travel Manager	Travel Specialist							
Others								
Initial Local Fact-Finding Stage	<div style="border: 1px solid black; padding: 5px;"> <p>Core Group</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Travel Manager</td> <td style="width: 50%; padding: 5px;">Travel Specialist</td> </tr> <tr> <td style="width: 50%; padding: 5px;">Travel Agency Representative</td> <td style="width: 50%; padding: 5px;">Others</td> </tr> </table> </div>	Travel Manager	Travel Specialist	Travel Agency Representative	Others	<ul style="list-style-type: none"> • Lead determines whether any travelers are affected • Attempt to contact traveler(s) using information from People Tracker and traveler profile and offer assistance if required 		
Travel Manager	Travel Specialist							
Travel Agency Representative	Others							
Expert External Resources Review Stage	<div style="border: 1px solid black; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Security Provider</td> <td style="width: 50%; padding: 5px;">Other Experts / Providers</td> </tr> </table> </div>	Security Provider	Other Experts / Providers	<ul style="list-style-type: none"> • Travel Agency also reviews pre-agreed reports and reports finding back to core group • Lead contacts security provider and/or other third-party provider if required 				
Security Provider	Other Experts / Providers							
Assessment and Management Stage	<div style="border: 1px solid black; padding: 5px;"> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Core Group</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">Travel Manager</td> <td style="width: 50%; padding: 5px;">Travel Specialist</td> </tr> <tr> <td style="width: 50%; padding: 5px;">HR Manager</td> <td style="width: 50%; padding: 5px;">Business Continuity</td> </tr> <tr> <td style="width: 50%; padding: 5px;">Risk Management</td> <td style="width: 50%; padding: 5px;">Others</td> </tr> </table> </div> <div style="text-align: center; margin-bottom: 10px;"> <p>Advisory \updownarrow Notification</p> </div> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <p>Selected pre-assigned internal manager</p> </div> </div>	Travel Manager	Travel Specialist	HR Manager	Business Continuity	Risk Management	Others	<ul style="list-style-type: none"> • Lead identifies appropriate email template, modifies appropriately, and sends to selected associates to notify them of the status of travelers • If determined that an associate might be affected the lead immediately informs VP-Human Resources with name and any specifics that can be furnished (e.g. it can only be known if associate was ticketed but not if actually on board a specific flight) <p>NOTE: Names of affected associates should only be given to the VP of HR</p>
Travel Manager	Travel Specialist							
HR Manager	Business Continuity							
Risk Management	Others							

Source: Based on model developed by The Capital Group of Companies

Acknowledgements

Advito would like to thank interviewees from the following organizations, whose expertise provided much of the content of this white paper:

ASI Global/MEDEX

ASIS International

BizJet Security

DuPont

Hewitt Associates

ijET Intelligent Risk Systems

ING

International SOS

Ministry of Justice (U.K.)

Mondial Assistance

PricewaterhouseCoopers UK

The Capital Group of Companies

Copyright 2009 by Advito. This publication may be reproduced in whole or in part or in any form for educational or non-profit services without special permission from the copyright holder, provided acknowledgement of the source is made. No use of this publication may be made for resale or any other commercial purpose without written permission of the copyright holder.



For more information on travel risk management, please contact:

ADVITO

1505 LBJ Freeway,
Suite 325
Dallas
Texas 75234

www.advito.com

advice@advito.com

About Advito

Advito provides travel-management advisory, procurement and outsourcing services that guide clients through a complex travel environment. Advito's focus on consulting delivers proven value, unbiased counsel and a customized approach for every client and every engagement, together with industry expertise and access to data to drive quantifiable decision-making. Advito is headquartered in Dallas, Texas, and London, Great Britain, and operates in key business markets around the world. Advito is an independent operating unit of BCD Travel, the world's third-largest travel-management company, owned by BCD Holdings N.V.

About BCD Holdings N.V.

BCD Holdings N.V., a Dutch family-owned company founded in 1975 by John Fentener van Vlissingen, is a market leader in the travel industry. The BCD Holdings' companies are: BCD Travel (global corporate travel management), Park 'N Fly (off-airport parking), TRX (travel transaction processing and data integration services) and Airtrade (leisure travel). The company employs approximately 15,000 people and operates in more than 90 countries with total sales, including franchising, of US\$ 15 billion. For more information visit: www.bcd-nv.com.