Best Practices for Implementing a Travel Risk Management Program

WorldAware®

Table of Contents

Executive Summary

Each time an employee travels, he or she is exposed to a range of personal health, safety, and security risks. At the same time, legal trends continue to shift the burden of mitigating these risks squarely onto employers. To address this critical issue, organizations must take a comprehensive approach toward protecting themselves and their travelers. In 2008, the Global Business Travel Association (GBTA) partnered with WorldAware to develop the Travel Risk Management Maturity Model™ (TRM3™). This risk management assessment tool continues to help organizations evaluate opportunities to improve their programs today.

Travelers and their employers continue to face new and growing threats while integrating rapidly changing technologies. Organizations today must simultaneously ensure compliance with industry guidelines, stay within budget, and meet client expectations. These pressures are driving industry leaders to plan across traditional functional boundaries and take an enterprise-wide approach toward travel risk management.

> Organizations must simultaneously ensure compliance with industry guidelines, stay within budget, and meet client expectations.

This document discusses travel risk management; details how the TRM3 assessment can serve as the basis for assessing any travel risk management program; and provides structured guidance for improving an organization's travel risk management program.

The objective of any risk management program is to mitigate risk to an acceptable level consistent with business objectives, governmental regulations, and the prevailing standard of care for an industry. A successful program will not only reduce the frequency and severity of incidents but also enable better management of the costs associated with response, recovery, lost productivity, and liability. Effective risk management ensures that a company is not at a competitive disadvantage. Organizations need a method to objectively benchmark their risk management programs; TRM3 provides such a method.

Travel Management

Before evaluating travel risk management (TRM) program, organizations must possess a solid understanding of TRM as a discipline. Like most aspects of business, travel risk does not come in a neatly bundled package. Risks to travelers and their employers begin when travelers leave the office and continue into the airport, hotel, surrounding community, and all points in between.

Dramatic examples of such risks include the Brussels bombings in the airport and metro stations (March 2016), hotel hostage crisis in Mali (November 2015), devastating earthquake in Nepal (April 2015), terrorist attacks on the Charlie Hebdo offices in Paris (January 2015), and continued political unrest in the Middle East and North Africa. Less dramatic, but no less disruptive, events include a nearly month-long general strike affecting aviation, rail, and maritime transport in France, Super Typhoon Nepartak spawning floods in East Asia, Zika virus and Chikungunya outbreaks in South America, and an escalating nationwide strike in Colombia.

Risks to travelers and employees begins when they leave the office and continue into the airport, hotel, surrounding community, and all points in between.

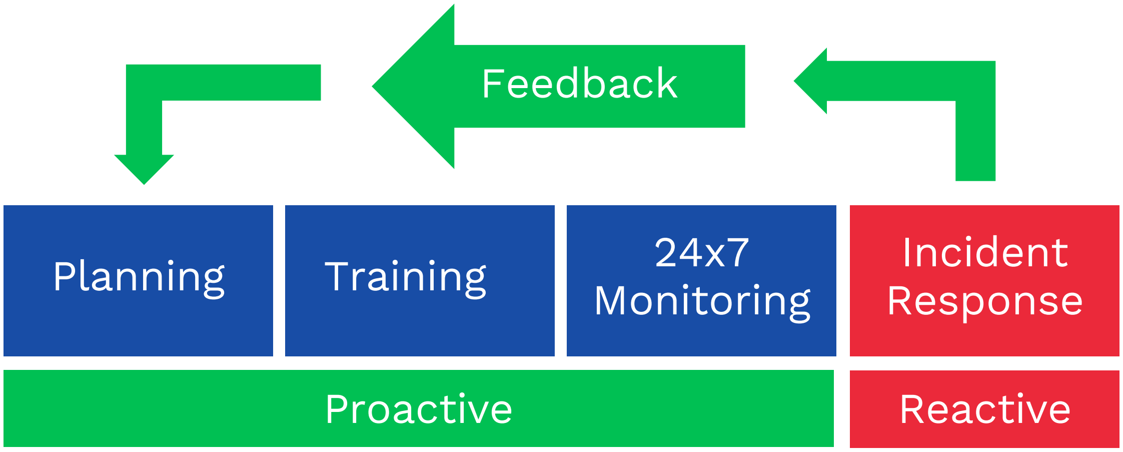
Disruptive events such as these can cost firms hundreds of thousands–even millions of dollars to respond and recover. For example, the average cost of a medical evacuation for an employee traveling abroad is $25,000–$30,000 USD. As one frequent business traveler recounts, during a business trip to a trade show, he spent nearly $2,000 USD to get a single piece of medical equipment through customs in Brazil simply because he was unaware of the requirement to register the unit in the U.S. before flying south. Such seemingly minor and routine disruptions add up.

The Global Business Traveler Association (GBTA) estimates the average cost of a three-day international business trip at more than $4,000 (USD). Organizations increasingly recognize not only the need to control travel costs but also to protect the investment that business travel represents—most significantly, employees who are traveling or on assignment. The impact and financial cost of employee downtime can be crippling to an organization, and the actual loss of an employee is beyond calculation. Proactive measures that reduce the frequency and severity of incidents help avoid response and recovery expenses as well as reduce potential liability.

Defining Travel Risk Management

TRM means a lot more than reacting quickly and efficiently to events as they unfold. In fact, the only reactive component of a sound TRM program is incident response. All other components (policies and procedures; training; 24x7 monitoring, including traveler tracking; and feedback) must be planned, implemented, and practiced before travel begins. By establishing a continuous process loop and training employees to follow it, all manner of risk (not only travel-related risk) can be significantly mitigated.

Basic TRM Program Building Blocks



We define "business travel" as any time an employee represents his/her organization away from home, either domestically or abroad. Travel can range from a drive to a facility in another city to a long-term assignment in another country. Expatriate assignees (long-term assignments) face more potential threats on an ongoing basis than do average travelers and as such their risk profile is significantly higher. Any time an employee is operating internationally, whether on travel or assignment, there are risks.

Travelers can face many different threats and hazards, including the trip to the airport, petty crime, and terrorism. However, threats are no longer risks if made irrelevant or properly mitigated. To this end, we define "risk" as:

Threat – Mitigation = Risk

However, risk management is not a formula. It's a process, comprising the following steps:

1. Identify relevant threats (threat environment).
2. Evaluate threats in relation to a traveler's profile (relevance).
3. Set an acceptable level of risk for the organization and employee (risk appetite).
4. Implement mitigation strategies that reduce threats to an acceptable risk level (mitigation).
5. Monitor for any changes in threats or a breakdown in the mitigation strategy (monitor).
6. Respond to an incident when it occurs (respond and recover).

Understanding the relationship between threat, mitigation, and risk in this way underscores the point that implementing a comprehensive, proactive TRM program is not a standalone project; it is a continuous, 24x7 process.

Understanding the relationship between threat, mitigation, and risk underscores the point that implementing a comprehensive, proactive TRM program is a continuous 24x7 process.

Building a Travel Risk Management Program

Using this risk management model, we can begin to depict a top-level view of an optimized TRM program. Although most organizations have some level of emergency assistance (typically travel and medical) for their travelers, they can no longer afford to react to travel problems merely. Travel risk needs to be actively managed. This means being proactive in helping employees avoid travel problems.

The following is an outline of the five key components of a proactive total TRM program.

Planning: An organization needs to define its overall TRM strategy, linking TRM policies to key organizational goals. This means determining how the TRM program will integrate with local crisis management plans (CMPs) and business emergency plans (BEPs). The main objective in this phase is to plan now so that the organization can do more than simply react later. There are a wide range of questions to consider during the planning phase such as, *"What is the company's response if an employee is kidnapped or killed," "How will the company evacuate employees in an emergency," and "What if an employee becomes seriously ill while traveling?"* These are all incident types that should be addressed during the planning phase.

Training: The purpose of training (TR) is to develop employees' skills and knowledge so they can perform their roles effectively and efficiently. In this whitepaper, we identify three specific areas of training that should be addressed: (1) traveler training, (2) travel advisor training, and (3) crisis management team training.

24x7 Monitoring: Systems and staff need to be put in place to provide real-time monitoring of potential threats to travelers worldwide. Through automated itinerary and assignment monitoring, the WorldAware TRM program notifies clients of any high-risk trips or assignments. When a threat is determined, getting this relevant information and possible mitigation strategies into the hands of the traveler or an advisor is critical. With advanced notification, many problems can be avoided.

Incident Response: Employees need to have someone to contact day or night for help in cases of emergencies. An optimized TRM program should be integrated into an organization's overall operating risk management (ORM) program. The resulting ORM program should include a single emergency hotline service for any issue or emergency impacting travel, facilities, and/or supply chains.

Understanding that no single internal resource or response vendor can handle every incident type in every location around the world, WorldAware has developed a command center infrastructure and incident management system to coordinate multidisciplinary response from multiple vendors. This system is customized for every organization and performed under the direction of the organization's crisis management team (CMT) or incident management team (IMT). For the organization, this solution enables global awareness of any incident that may impact people or operations. For an employee, it provides one phone number that can be used worldwide for any problem.

Events such as violent civil unrest across the Middle East and North Africa as well as terrorist attacks in Paris and Brussels, and the devastating natural disasters in Nepal, underscore the need for an integrated incident management approach that extends beyond travel. During and following these events, corporate travel departments learned, again, that they are only part of a robust incident response that requires integration with several departments across their organization.

Organizations with well developed, integrated incident management plans, processes, and procedures fare significantly better than those with underdeveloped and/or disjointed programs.

Feedback: Following any incident, it is essential to have an after-action review (AAR). The after-action review asks: *"Could the problem have been prevented in the first place?"* And if not, *"Could the incident have been handled more effectively?"* If the answer to either of these questions is "Yes," then a modification of existing policies, plans, procedures, or mitigation strategies is required.

This feedback process could be included in a short survey after each trip. This feedback would provide valuable information about the organization's travel program and capture any issues or concerns employees might have. Risk management must be an ongoing process under continuous improvement.

Legal Obligations

There are also legal imperatives to implementing a comprehensive TRM program: duty of care, duty to disclose, and standard of care. These legal standards apply whether the organization is a corporation, governmental agency, or a nongovernmental organization.

Duty of Care

This is the legal responsibility of an organization to do everything "reasonably practical" to protect the health and safety of employees. Though interpretation of this language will likely vary with the degree of risk, this obligation exposes an organization to liability if a traveler suffers harm. Some of the specific elements encompassed by duty of care include:

- A safe working environment–this extends to hotels, airlines, rental cars, etc.
- Providing information and instruction on potential hazards and supervision in safe work (in this case, travel).
- Monitoring the health and safety of employees and keeping good records.
- Employment of qualified persons to provide health and safety advice.
- Monitoring of conditions at any workplace (including remote locations) under the organization's control and management.

Duty of care is a powerful principle determining corporate responsibility. It is used predominantly in the United States, though similar standards exist in other countries, including the United Kingdom and France. Today, duty of care is incorporated within the policies, procedures, and practices of many industry leaders around the world.

Legislation is being enacted to enforce the duty of care concept. In the United Kingdom, the Corporate Manslaughter and Corporate Homicide Act of 2007 has been used to successfully prosecute a U.K. company in the death of an employee. A lawsuit involving a kidnapping and a non-governmental aid worker in Sudan has been filed in the U.S. Clearly, duty of care is becoming the standard by which organizations will be judged in the event that harm befalls an employee.

One simple example of how an organization might be exposed to liability via duty of care obligations is through a preferred hotel program. In a preferred hotel program, a company negotiates favorable rates with specific hotels and then asks or requires employees to stay at these properties. However, if an employee staying at one of these facilities is attacked while out jogging, what is the potential liability to the company? How does that change if the hotel bordered a high crime area that was fairly well known as a dangerous locale? A robust TRM program would take into account hotel safety and security factors as part of an overall effort to meet duty of care standards. The security aspect of a preferred hotel program could be captured as part of an RFP due diligence process. In fact, the GBTA standard hotel RFP has a safety and security module that can be easily incorporated in such a process.

Duty to Disclose

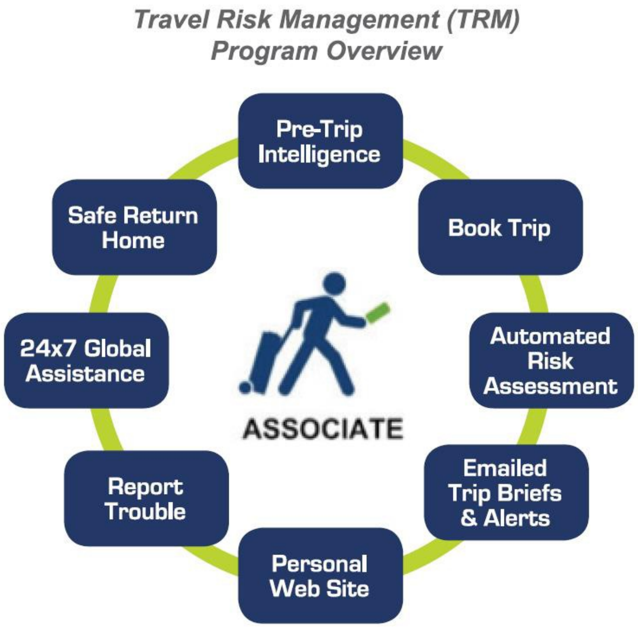
This concept focuses on an organization's responsibility to monitor and disclose potential risks. For example, if there is ongoing civil unrest in a city, an organization has an obligation to disclose this to travelers so that they can make an informed decision about whether or not to take the trip.

An organization could claim that it did not know of this risk, but then a court would likely ask, *"Should the organization have known?"* Given the number of available sources of information, including free sources such as government travel warnings and cable news as well as relatively low-cost services such as those offered by WorldAware and others, a claim of ignorance may not hold up in court.

Beyond limiting an organization's potential exposure to liability, duty to disclose, if implemented as part of an overall TRM program, can become an important way for organizations to support their bottom line. For example, let's say a major demonstration is scheduled for the city center of Rome. An employee books a trip, not knowing that the protest is planned for the day that she is meeting with clients and prospects. She arrives, finds traffic at a standstill, and misses the scheduled meetings. While she faced no personal threat, the company just spent thousands of dollars for little or no return. Several weeks later the company must spend thousands more to send her to Rome again to complete the unfinished work.

Meeting an organization's duty to disclose in a way that not only limits liability but also helps employees accomplish their mission should be a goal of a TRM program.

A mature, well-structured travel authorization process (TAP) that factors in travel expenses, business needs for travel, the company travel policy, as well as travel risk is another component of the duty to disclose concept. An automated and fully integrated TAP can help ensure that the right information reaches the right people. This allows for informed decision making that is disclosed to all appropriate stakeholders. These stakeholders may include the traveler, individuals authorizing travel, and supporting vendors (e.g., travel management companies; security providers; hoteliers; medical response providers; ground transportation).



Standard of Care

Simply put, if an organization's peers have implemented programs to protect staff, it can be held liable for not providing a similar level of care. Many organizations are using services like those offered by WorldAware to capture itineraries (traveler tracking), provide pre-trip information (risk disclosure), keep travelers informed of new risks, and provide emergency assistance support. A GBTA survey showed that approximately 80% of companies had some level of a "traveler tracking" program.

Standard of care is a moving target, subject to change as new practices are adopted within an industry. An organization must show that it was not reasonably practical to do more or that management did in fact take "reasonable precautions and exercised due diligence" to meet its standard of care obligations. As a way to meet this evolving requirement, WorldAware has seen more organizations opting to push risk disclosure to employees rather than requiring employees to pull such information from a website. Pushing relevant information to employees can result in eight times greater utilization than pulling. Knowing what measures similar organizations are taking is an important determinant of standard of care and the risk of any potential liability.

Other Obligations

Several other laws and regulations also continue to shape the legal obligations of organizations when it comes to travel. The Foreign Corrupt Practices Act (FCPA) has been in effect in the U.S. since 1977, but in recent years has been used in a spate of convictions that indicate a stringent approach by the courts. Similarly, legal experts have argued that the U.K. Bribery Act enacted in 2010 is even more severe than the FCPA. Given these legal trends, it is in the best interest of every organization to ensure that appropriate standards are vigilantly maintained.

Business Impact

As convincing as these legal points are in supporting the need for a comprehensive TRM program, the practical reasons are even more compelling. Organizations spend significant sums on travel and management of employees on assignment. It is both prudent and cost-effective to protect the safety, health, and productivity of employees as they work to achieve an organization's objectives. Implementing a robust TRM program with a focus on "trip purpose" will significantly help reduce potential liability in the event of an incident. More and more it is becoming the norm that:

- A board mandates a risk management program; or
- Potential clients demand to see a risk management program as part of the due diligence process.

A focus on "trip purpose" will significantly help reduce potential liability in the event of an incident.

Role of Technology

The drive for more granular traveler tracking using mobile technology is particularly relevant to the legal obligations mentioned above. As organizations determine their level of standard of care, they look to standard practices in their industry for guidance. One of the most significant trends has been the growth in mobile tracking services. While mobile tracking is prevalent in certain sectors, especially among organizations with operations in high-risk areas, other types of organizations have begun exploring such services to protect their employees under more mundane travel circumstances. Meanwhile, vendors have been expanding ways to provide such services to mainstream clients.

Another significant development has been the rapid growth in the social media space, both in terms of technological advances and potential applications. These advances pose both challenges and opportunities to professionals in the travel industry as well as partners in operational risk management. Two areas where the efficient use of social media can yield benefits are:

- **Program Communications** – Using social media to communicate an organization's TRM program structure, policies, and benefits to employees and other relevant constituents.
- **Emergency Communications** – Tools such as popular search engines, social networks, and microblogs are becoming some of the most-used communications technologies during crisis situations. Potential uses are multiple; social media can be used to provide situational awareness in a crisis, establish communications with employees that cannot be reached via traditional means, and communicate status updates to relevant constituents.

Growth of technology, especially on the mobile front, has forced multinational organizations to address concerns around the protection of intellectual property, data privacy (both for the organization and the individual employee), and standards for devices and applications being used.

Travel Risk Management Maturity Model (TRM3)

The Travel Risk Management Maturity Model (TRM3) is a way to develop and refine an organization's processes with respect to its TRM program.

In general, a maturity model describes the characteristics of effective processes. A maturity model provides:

- A place to start.
- Benefits of a community's prior experiences.
- A common language and a shared vision.
- The framework for prioritizing actions.
- A way to define what improvement means for an organization.

A maturity model such as TRM3 can be used as a benchmark for assessing different organizations for equivalent comparison. It describes the maturity of an organization based on an evaluation of key process areas (KPAs) that are required to implement and support a successful TRM program.

It should be noted that the TRM3 is a model, not a process. The model describes the characteristics of an effective TRM program while each KPA addresses the specific processes required to implement the program. The TRM3 is designed to guide efficient and effective improvement across multiple process disciplines within an organization.

> The TRM3 is designed to guide efficient and effective improvement across multiple process disciplines within an organization.

Maturity Levels

In defining the TRM3 maturity levels, we have borrowed heavily from the framework used in the Software Engineering Institute Capability Maturity Model Integration (CMMI). As in the CMMI, the TRM3 organizes the evolution of an organization's maturity into five maturity levels. Each level lays successive foundations for continuous improvement. These levels also help an organization prioritize improvement efforts. The table below highlights the characteristics of the five maturity levels as well as the primary process changes made at each level.

The TRM3 model has been designed to evaluate the ten key process areas at each level. When rating an organization's maturity, it is important to use the lowest KPA rating as the overall organizational rating. For example, an organization's Policy/Procedures KPA may be at Level 4 and the Risk Mitigation KPA may be at Level 2. Such a situation would result in TRM3 rating of Level 2.

For an organization to be rated at a given maturity level, each of the KPAs needs to be rated at that level or higher. Any KPAs that fall short should immediately become an organization's topmost priority areas for improvement as management works towards the next level. Beyond that, management should prioritize its effort by KPAs that will provide the greatest return for the TRM program.

If a program is rated at Level 1, the organization is at substantial risk and could incur significant liability for not meeting basic duty of care for travelers. General Counsel should help to attain the resources needed to implement a risk management program.

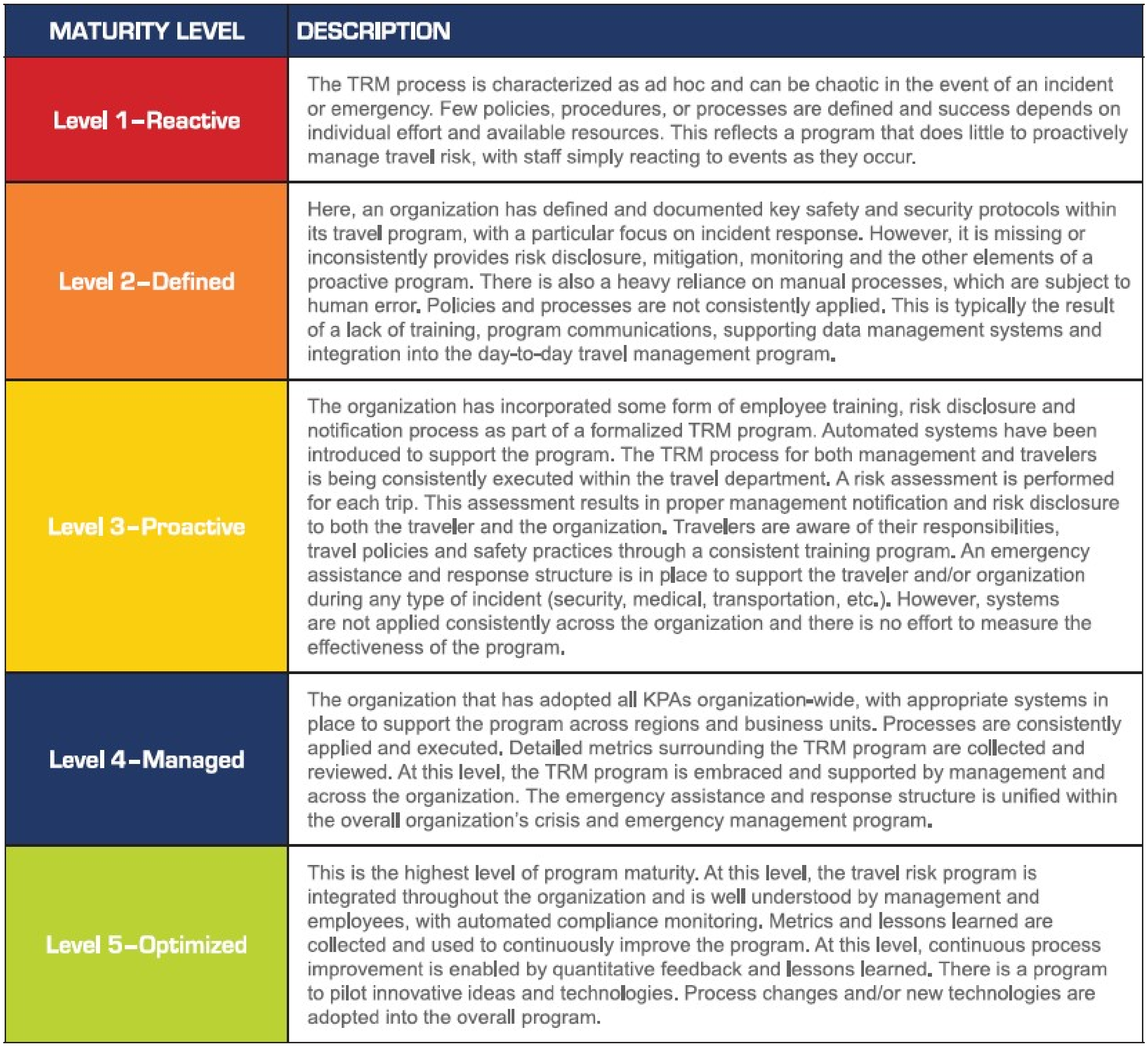
It's not unusual to have a Level 2 program rating. Many organizations have the basic elements of a sound TRM strategy but fail to apply and communicate them consistently. At Level 2, an organization is typically prepared to act if something happens but does little or nothing to help the traveler and organization avoid a problem in the first place.

While most organizations should meet a Level 3 standard of care, many do not. At this level, an organization is doing what it can to be prepared for and manage risks faced by travelers. The biggest hurdles are instituting the program across the organization and ensuring that travelers are utilizing the tools provided to avoid incidents.

To date, we have seen less than a handful of organizations that have achieved Level 4. To attain this level, a TRM program needs to be fully integrated into the overall enterprise risk management program. Data systems would consistently implement and monitor policies. Mitigation is consistently applied; employees and management are active users of the system, and a formal training and communications program has been instituted.

Level 5 means a program that is not only world-class, but that a process improvement program exists covering all 10 KPAs. In each area, metrics are collected, feedback from travelers is analyzed, and incident lessons are learned to optimize and drive program effectiveness. Exercises and drills are conducted to ensure that everyone involved understands their role and responsibility within the organization.

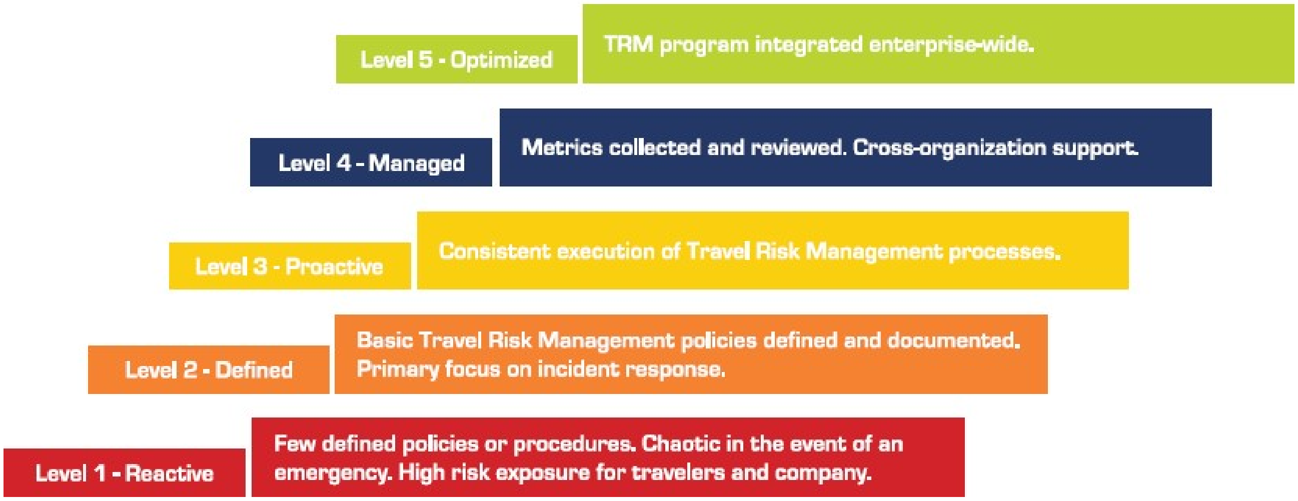
TRM3 Maturity Levels



MATURITY LEVEL	DESCRIPTION
Level 1–Reactive	The TRM process is characterized as ad hoc and can be chaotic in the event of an incident or emergency. Few policies, procedures, or processes are defined and success depends on individual effort and available resources. This reflects a program that does little to proactively manage travel risk, with staff simply reacting to events as they occur.
Level 2–Defined	Here, an organization has defined and documented key safety and security protocols within its travel program, with a particular focus on incident response. However, it is missing or inconsistently provides risk disclosure, mitigation, monitoring and the other elements of a proactive program. There is also a heavy reliance on manual processes, which are subject to human error. Policies and processes are not consistently applied. This is typically the result of a lack of training, program communications, supporting data management systems and integration into the day-to-day travel management program.
Level 3–Proactive	The organization has incorporated some form of employee training, risk disclosure and notification process as part of a formalized TRM program. Automated systems have been introduced to support the program. The TRM process for both management and travelers is being consistently executed within the travel department. A risk assessment is performed for each trip. This assessment results in proper management notification and risk disclosure to both the traveler and the organization. Travelers are aware of their responsibilities, travel policies and safety practices through a consistent training program. An emergency assistance and response structure is in place to support the traveler and/or organization during any type of incident (security, medical, transportation, etc.). However, systems are not applied consistently across the organization and there is no effort to measure the effectiveness of the program.
Level 4–Managed	The organization that has adopted all KPAs organization-wide, with appropriate systems in place to support the program across regions and business units. Processes are consistently applied and executed. Detailed metrics surrounding the TRM program are collected and reviewed. At this level, the TRM program is embraced and supported by management and across the organization. The emergency assistance and response structure is unified within the overall organization's crisis and emergency management program.
Level 5–Optimized	This is the highest level of program maturity. At this level, the travel risk program is integrated throughout the organization and is well understood by management and employees, with automated compliance monitoring. Metrics and lessons learned are collected and used to continuously improve the program. At this level, continuous process improvement is enabled by quantitative feedback and lessons learned. There is a program to pilot innovative ideas and technologies. Process changes and/or new technologies are adopted into the overall program.

The next section provides an overview of the KPAs.

TRM3 Maturity Levels (2)



Level 5 - Optimized: TRM program integrated enterprise-wide.

Level 4 - Managed: Metrics collected and reviewed. Cross-organization support.

Level 3 - Proactive: Consistent execution of Travel Risk Management processes.

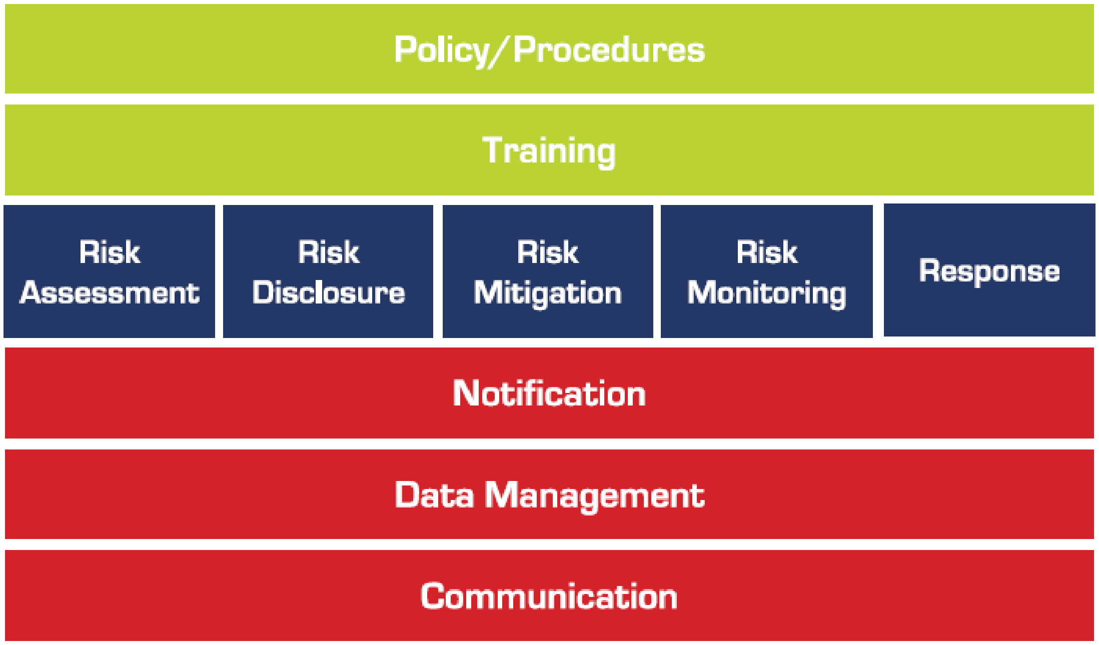
Level 2 - Defined: Basic Travel Risk Management policies defined and documented. Primary focus on incident response.

Level 1 - Reactive: Few defined policies or procedures. Chaotic in the event of an emergency. High risk exposure for travelers and company.

Key Process Areas

Key Process Areas (KPAs) are the key components of any TRM program. At the lower levels of program maturity, these KPAs would be implemented within the travel program. At the higher levels, these processes are embraced and integrated into broader organizational risk management and business resilience programs.

Key Process Areas (KPAs)



Policies and Procedures

The purpose of the Policy/Procedures (PP) area is to focus attention on the process of developing and maintaining policies and procedures in support of TRM.

To reach maturity in the Policy/Procedures KPA, organizations must ensure that policies are well defined and documented, broadly integrated within organizational risk policies, implemented within the overall travel process, measured and monitored for compliance, and supported by a continuous improvement process. Maturity in the Policy/Procedures KPA means developing, implementing, and maintaining policies and procedures. Note that this KPA does not refer to the specific policies and procedures themselves.

Typical risk management policies include the use of private aviation, limitations on the number and type of employees on the same flight, prohibited travel destinations, approval process to high-risk destinations, etc. All TRM policies and procedures should address several important areas, including vetting of vendors and suppliers, business continuity of travel operations and call centers, and incident and emergency response protocols. These policies and procedures should be developed as part of the other KPAs defined below.

> To reach maturity in the PP KPA, organizations must ensure that policies are well defined and documented, integrated, implemented, and monitored.

Training

The purpose of Training (TR) is to develop employees' skills and knowledge so they can perform their roles effectively and efficiently. The three specific areas of training that should be addressed are: (1) traveler training, (2) travel advisor training, and (3) crisis management team training.

- **Traveler Training** addresses basic pre-travel knowledge areas. This training covers all the essential issues from pre-trip planning to skills on the road, and decompressing when a traveler gets home. In addition, an organization can offer a wide variety of enhanced courses on traveling to high-risk destinations, executive protection, surveillance detection, defensive driving, etc.
- **Travel Professional/Advisor Training** covers the systems and processes used to implement the TRM program. The professionals in an organization – in particular travel, security, and human resources staff– need to know what is expected of them to prevent or handle an emergency.
- **Crisis and Emergency Management Team Training** focuses on simulations and drills to ensure that crisis management plan (CMP) and procedures are exercised, and that people know what is expected of them in an emergency.

The training process involves several activities. It starts with identifying the training required as well as who should conduct and receive that training. The process also includes developing the training program and modules and having a consistent process to ensure that the training is delivered and documented.

For example, if a traveler is going to a high-risk destination, the organization should ensure that the employee has basic health and safety training as well as training around traveling to a high-risk destination. If the employee will be on a long-term assignment (expatriate), the training should be tailored to unique issues that may be encountered under such circumstances. There is no requirement that these training modules be formal or flashy. The only requirement is that the proper policy, health, safety, and related information are conveyed to the traveler prior to departure. This can be done over the phone, face-to-face, in periodic classroom sessions, or online.

Risk Assessment

The purpose of Risk Assessment (RA) is to ensure that each trip or assignment is evaluated and scored for risk as an input to the overall decision process.

Risk assessment is the foundation of the overall TRM program and should be conducted on every trip, assignment, and special event. For example, Washington DC, London, New Orleans, and Madrid may not be considered higher-risk destinations. However, each of these cities has had elevated risk ratings due to natural disasters, terrorist events, or civil unrest and protests. While traveling to New Orleans would normally be low risk, if forecasters are predicting a hurricane, both the employee and the organization need to be aware of that threat and develop a mitigation plan to address it.

Given the changing threat environment around the world, the risk assessment program must take into account both the intrinsic threat level for a destination and any dynamic threats that may elevate the risk of operating in that area over some period of time. This is especially true for employees who are traveling or assigned to a location for an extended time frame.

> Risk assessment is the foundation of the overall TRM program and should be conducted on every trip, assignment, and special event.

Risk Disclosure

The purpose of Risk Disclosure (RD) is to produce information related to the risk assessment so that all relevant parties are aware of the potential threats that may be encountered.

As an output of the Risk Assessment process, the organization needs to develop processes to ensure that the appropriate people are aware of the current threat environment. One model is to ensure that employees get basic health and safety information on each trip. If the trip risk assessment level exceeds a defined threshold, then others within the organization should be notified of the potential exposure. Typically, the people to be notified include travel, risk/security leaders, as well as the line manager.

The Risk Disclosure process should ensure that each stakeholder understands the nature of the threat, how it may impact the employee and/or organization and what should be done to eliminate or minimize the risk.

Risk Mitigation

The purpose of Risk Mitigation (RM) is to develop strategies and solutions that will result in a level of risk that is acceptable to all parties (i.e., the employee, the manager and the company).

Identifying potential threats is not enough. The organization and employee need to understand how relevant a threat is to the trip and business being conducted. From there, both standard and ad hoc mitigation strategies need to be developed to reduce the resulting risk to a level such that both the employee and the organization are comfortable conducting the trip. If an acceptable level of risk cannot be achieved, then alternatives such as canceling or rescheduling the trip can be explored.

Risk Monitoring

The purpose of Risk Monitoring (RMON) is to develop real-time monitoring of world events for potential threats to personnel.

Each organization needs to have an around-the-clock process to monitor the current threat environment across all segments of the trip. This includes travel destinations, modes of transport (e.g., air; rail; sea ports), hotels, transportation carriers, etc. Once a new threat is identified or any existing threat level changes, that new information must be captured and fed into both the Risk Assessment and Notification processes.

Once a new threat is identified or an existing threat changes, that new information must be fed into the Risk Assessment and Notification processes.

Response

The purpose of Response (RP) is to provide travelers with an easy-to-use process for reporting problems and getting assistance.

The Response KPA addresses the reactive component of the overall program. An organization needs to be prepared for an event or incident. Having proper response plans and protocols in place with the appropriate resources is the foundation of the Response KPA; however, integrating this into the Training KPA and the Communication KPA are what allow an organization to reach full Response maturity.

Notification

The purpose of the Notification (NT) process is to ensure that the appropriate people are informed of any relevant travel risk information before, during, or even after a trip so they can make rapid and thoughtful risk-related decisions.

There are many elements of this process, such as relating personnel to assets (based on role, organization, etc.), capturing and maintaining accurate contact information, the actual notification process and capturing performance metrics.

Data Management

The purpose of Data Management (DM) is to establish and maintain the data required to monitor and manage a robust TRM program. The Data Management KPA addresses the overall process of identifying, collecting, storing, accessing, and maintaining this information. This KPA is responsible for assembling the data that represents a community's prior experience.

The breadth and depth of information collected and maintained to support a comprehensive TRM program can be significant for a program of any size. This information includes personnel contact profiles, trip itineraries, long-term assignments, threat information, destination (country/city) information, organizational structure, etc. A critical part of this KPA is integrated data quality assurance processes that ensure data is accurate and properly archived for use in audits and risk management decisions.

Communication

The purpose of Communication (CO) is to ensure that all stakeholders understand the TRM program and their role within it.

This KPA focuses on the organization's responsibility to properly communicate the program and all of its elements to each constituent group. These groups include employees, management, senior management, emergency and crisis management teams, contractors, families, and external entities such as vendors, suppliers and channel partners.

Travel Risk Management Maturity Model (TRM3) Assessment Process

Conducting a TRM3 assessment can help determine which TRM3 maturity level best describes an organization's TRM program. An organization can conduct a TRM3 assessment at a high level – a quick internal assessment through interviews – or at a deeper level with an in-depth review involving surveys of key stakeholders and tangible evidence confirming that polices or procedures are in place. This comprehensive TRM3 assessment should include a detailed roadmap on how to move the program to the desired level.

Quick Internal Assessment Process

If an organization is interested in a fast, high-level assessment of its TRM program, it can very quickly interview and/or survey key people involved in the travel process. Using the KPA rating matrix below, each survey participant selects the level that best describes his or her assessment of the organization's TRM program for each KPA.

A simple internal assessment would look for agreement for each KPA. For example, if each of four individuals rate the Policy/Procedures KPA at Level 2 and a fifth rates it at Level 3, then collectively, all individuals rate the Policy/Procedures KPA at Level 2 or higher. Below we address the value of analyzing discrepancies in the ratings.

In-Depth Assessment Process

The next level of assessment is to look deeper into the program. Rather than just relying on individual assessments, the assessment process identifies and documents actual evidence that the KPA is being performed at a given level. This can be done by an internal team or through an independent assessment resource such as WorldAware or one of its approved consultants. This more formal assessment would collect input from all stakeholders, including senior and line management, functional department management (travel, HR, security, risk, etc.), support vendors, employees, and travelers.

This assessment focuses on any differences in assessment levels within a given area and between stakeholder groups. For example, a travel manager may rate the organization high in several KPAs, believing that policies and procedures are in place and are being followed. However, other members of the department may rate these areas much lower, knowing that some procedures are not being followed or are not being followed consistently.

Travel Risk Management Maturity Model (TRM3) Self-Assessment Tool

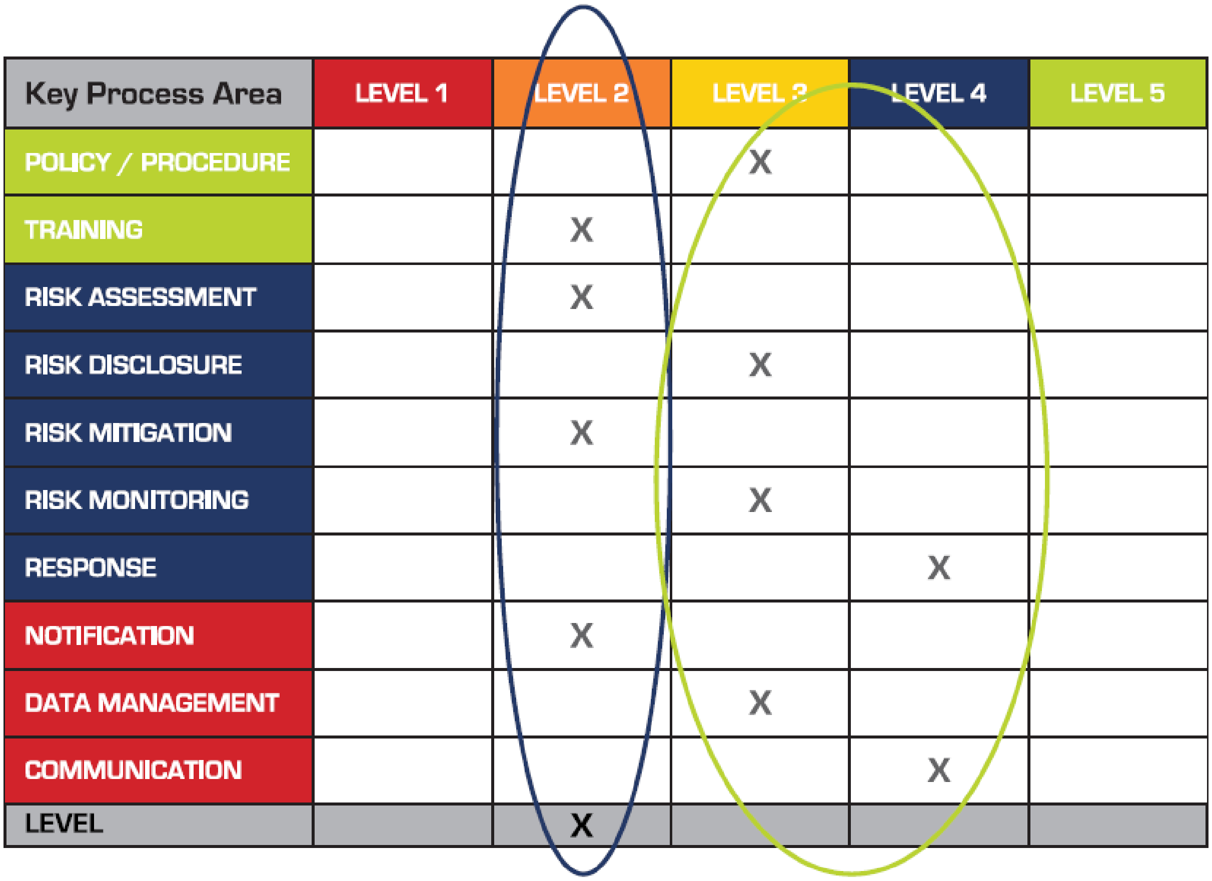
Careful attention should be paid to any differences in assessment levels for each KPA. Where there are discrepancies, the final rating level for each KPA should rely on objective evidence to support the rating.

The TRM3 assessment form at the end of this section provides a guideline in which to evaluate each key process area (KPA). Using the KPA Matrix, read the description for each level, then pick the level that best matches your TRM program. If you have nothing in place, rate that item as a "Level 1".

As shown below, mark the corresponding assessed level for the KPA in the assessment form. Complete this process for each of the KPAs.

Sample TRM3 Assessment Scoring

TRM3 Rating: Level 2 – Plus 6



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			

The lowest level rating across all KPAs is your TRM3 Level. In the example, this is Level 2. Then, count the number of KPAs with a level higher than the lowest level. This is your Plus number. In the example, there are 6 KPAs greater than Level 2. The Plus number indicates how close you are to achieving the next TRM3 maturity level.

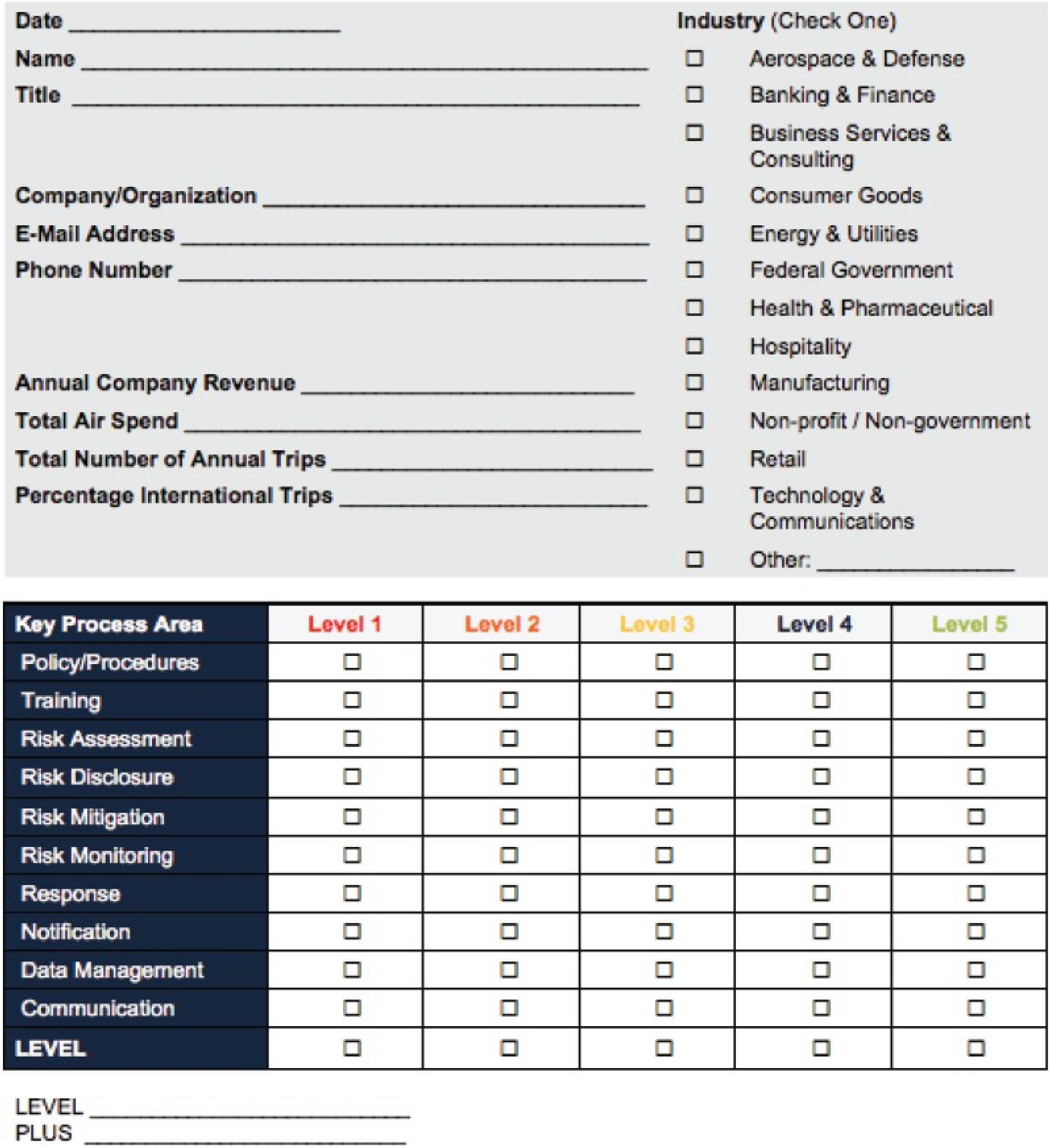
Key Process Areas (KPAs) Rating Matrix

	LEVEL 1 Reactive	LEVEL 2 Defined	LEVEL 3 Proactive	LEVEL 4 Managed	LEVEL 5 Optimized
Policy/ Procedures (PP)	No defined TRM policies or procedures to maintain them	Defined TRM policies, procedures; ad hoc implementation	Defined TRM 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 TRM	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	Training program includes an improvement process; metrics drive training effectiveness; training provided based on risk, location, and/or special situation
Risk Assessment (RM)	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 assessments 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 the trip	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 various 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
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 into 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 by 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	Process in place to continuously improve the response program; metrics and lessons learned drive response speed and effectiveness

Key Process Areas (KPAs) Rating Matrix (Cont.)

	LEVEL 1 Reactive	LEVEL 2 Defined	LEVEL 3 Proactive	LEVEL 4 Managed	LEVEL 5 Optimized
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 is 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 TRM	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 TRM 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 (CO)	No or ad hoc communication with stakeholders	Basic documented program around risk communications	Communication integrated into the travel business process; consistent processes used to distribute information	Organizational management engaged in TRM communications program; multi-level and multi-modal communications programs	Improvement process in place to capture and apply feedback and lessons learned; metrics are captured to support the improvement program

Travel Risk Management Maturity Model (TRM3) Assessment Form



Date ____________________

Name ____

Title ____

Company/Organization ______________________________

E-Mail Address ___________________________________

Phone Number ____________________________________

Annual Company Revenue __________________________

Total Air Spend __________________________________

Total Number of Annual Trips ________________________

Percentage International Trips ______________________

Industry (Check One)

- □ Aerospace & Defense
- □ Banking & Finance
- □ Business Services & Consulting
- □ Consumer Goods
- □ Energy & Utilities
- □ Federal Government
- □ Health & Pharmaceutical
- □ Hospitality
- □ Manufacturing
- □ Non-profit / Non-government
- □ Retail
- □ Technology & Communications
- □ Other: _______________

Key Process Area	Level 1	Level 2	Level 3	Level 4	Level 5
Policy/Procedures	□	□	□	□	□
Training	□	□	□	□	□
Risk Assessment	□	□	□	□	□
Risk Disclosure	□	□	□	□	□
Risk Mitigation	□	□	□	□	□
Risk Monitoring	□	□	□	□	□
Response	□	□	□	□	□
Notification	□	□	□	□	□
Data Management	□	□	□	□	□
Communication	□	□	□	□	□
LEVEL	□	□	□	□	□

LEVEL ________________________

PLUS ________________________

About WorldAware

WorldAware, Inc. provides intelligence-driven integrated risk management solutions that enable multinational organizations to operate globally with confidence. WorldAware's end-to-end tailored solutions integrate world-class threat intelligence, innovative technology, and response services to help organizations avoid threats, mitigate risk, and protect their people, assets, and reputation. Founded in 1999, WorldAware is a privately held company headquartered in Annapolis, United States with offices in London, Cape Town, and Singapore.

For more information, please visit www.worldaware.com.