JOURNEY MANAGEMENT | Utilising Security Movement Teams, effective planning, compliance, human rights, humanitarian law and security risk management

Peregrine
Risk Management

International organisations mobilise their workforce to support operational and business objectives. To achieve this, safely and securely, it is essential that journey management practices are adopted. The level and type of services required can be defined once a detailed threat and risk assessment has been conducted. Once the threat vectors and adversaries have been identified the appropriate means of transportation can be allocated.

When deciding what form of transportation is required it is also important to consider the following;

Criminality: are crimes such as carjacking and robbery prevalent. Does public transportation raise the likelihood of petty crime.

Terrorism: are terror attacks targeting vehicles, road networks and critical infrastructure.

Unrest: are protests likely to disrupt your scheduled journey management programme and route selection. Will checkpoints be deployed causing additional disruption or public transportation access delayed, denied or blocked.

Terrain, Weather and Road Conditions: is the vehicle selection suitable for the environment and terrain.

Driving Standards: is the localised driving standards safe enough to permit your people to use public transportation, self-drive services or unvetted security teams with no defensive driving experience.

Personnel: is the profile of your people, organisation or operational requirements likely to increase risk exposure and vulnerability.

Security Services

The following security services could be contracted to enhance your travelling personnel's safety whilst operating in new, unfamiliar, complex and high-risk environments.

Meet & Greet: Airport Meet & Greet services enable the swift collection of new arrivals and their safe return prior to departure.

Security Movement Teams (Private): Security Movements Teams (SMT) can be utilised for several reasons; the threat and risks posed are high, high-level executives may pose an increased risk due to their position or standing. In some high to extreme risk countries where terrorism is commonplace armoured vehicles could also be selected to enhance protection.

In-Country Security Agencies: In some regions, to complement an SMT, the use of localised security agencies is required. An example of this occurs when operating in countries like Nigeria where Mobile Police (MOPOL) are needed.

Incident Response 24/7 and Redundancy: To support security services it is always essential to understand what reactive controls can be deployed to support an incident, should one occur. It is therefore crucial that a clear understanding of capability and resources is understood prior to deployment. This can include; additional vehicles and types, Quick Reaction Force, reporting and communication mechanisms.

Utilising Security Providers

Unfortunately, the security industry struggles to enforce best practice and in most cases security providers are delivering fractured and non-compliant solutions to their clients. Any security company can profess to deliver the highest standard of solution but how is this independently validated and audited.

Without a robust security operations framework, a security provider is exposed, thus leaving your people exposed. This leads to bad practice, un-audited and tested security solutions, increased exposure to risk, unsafe and secure practices, corruption, licensing and compliance issues, unverified training and human rights breaches to name but a few.

The right way

There are two credible certification routes for private security companies to demonstrate to their clients that security operations are of paramount importance.

ISO 18788:2015: This standard is based upon the ethos of the United Nations Guiding Principles of Business & Human Rights. Certification provides clients, governments and communities with assurance that a robust and resilient Security Operations Management System (SOMS) has been implemented and certified. As a Private Security service provider and risk management specialist, certification to ISO 18788:2015 provides credibility, demonstrating effective Corporate Governance – from Board level, to physical delivery[1].

ANSI/ASIS PSC.1-2012: This standard demonstrates our commitment, conformance, and accountability to the principles outlined in the International Code of Conduct (ICoC) for Private Security Service Providers by providing a management system for quality of Private Security Operations. The PSC.1 standard, which builds on the historic Montreux Document and the International Code of Conduct for Private Security Service Providers (ICoC), was developed by ASIS International, in conjunction with the American National Standards Institute, Inc. (ANSI), in order to establish auditable criteria for managing the quality of private security services and ensure respect for human rights and legal obligations "in conditions where governance and the rule of law have been undermined by conflict or disaster". PSC.1 enshrines the protection of human rights within the industry's business practices and provide confidence in the quality and professionalism of security firms operating in fragile environments[2].

Security Operations Framework | ISO 18788:2015:

Risk Assessment: As per standard ISO 31000:2018 risk assessment methodology it is always important to understand the context of the security solution. Followed by;

- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment

Planning and Control: To ensure security services are delivered to the highest standard it is extremely important that the chosen security provider adheres to the following;

- Operates in-line with legal and regulatory requirements (home and host nation)
- All licenses are implemented, in-date and approved and issued by local government agencies
- Clear risk management controls with defined targets and objectives

Each provider must have a clear Mission Statement and embrace and adhere to International Humanitarian Law and Human Rights as driven by the International Code of Conduct Authority (ICoCA). In addition, all providers must enhance the security and well-being of those

[1] https://www.iso.org/obp/ui/#iso:std:iso:18788:ed-1:v1:en

[2] https://store.asisonline.org/management-system-for-quality-of-private-security-company-operations-standard-softcover.html

clients they are contracted to protect as well as respecting local communities and cultures.

Code of Conduct: Each member of the security risk management company, from the top down, must behave and act professionally at all times. This includes adherence to human rights, international humanitarian law and ethics.

Use of Force: Rules for the Use of Force are an integral component for the delivery of security operations. The Use of Force continuum must consider the following;

- Weapons authorisation and licensing
- Use of Force
- Less Lethal Force
- Lethal Force
- Use of Force in support of Law Enforcement
- Use of Force training

In addition to the Use of Force security providers must also consider Apprehension and Search Procedures which must be implemented should an incident dictate.

Not all security providers around the world will work or support Law Enforcement but if this is the case, consideration for support and detention operations need to be included within the operational functions provided.

Resources, Authority and Roles & Responsibilities: Selecting the right personnel is vital and it is important that the right vetting and background checks are conducted to ensure not only that the security members are appropriately qualified, but they are legally permitted to act as a security professional from a criminal perspective.

Each country is different and a clear understanding and process for the procurement of weapons and munitions must be enforced as per national and international law.

Defined roles and responsibilities are also required so that there is accountability throughout the delivery of security services. The use of appropriate uniforms and markings also requires consideration.

Journey Management: When utilising a security provider there must be a clear and defined scope of work which defines all deliverables and expectations. The level of security required is identified during the risk assessment phase to ensure the profile and configuration selected is appropriate to the threat environment.

Once the scope has been agreed a robust journey management programme should then be created to ensure the service runs smoothly and in accordance with business objectives, local and international law, and human rights.

Incident Management: The security provider should develop and implement a robust incident response process that enables quick and targeted contingencies to reduce the impact of any potential incident. This process must include risk communication strategies, reporting and recording of incident details.

Performance and Quality: As with any professional service it is imperative that the quality and performance of security services is continually tested, monitored, and reviewed. A credible provider will enforce a quality management system such as ISO 9001:2015 to ensure this is achieved.

The Solution

Peregrine Risk Management holds certification in ISO 18788:2015, ANSI/ASIS PSC.1-2012, ISO 9001:2015 and aligns to ISO 31000:2018. This has enabled Peregrine Risk Management to develop a compliant and robust Global Security Network which ensures our security providers are either certified to ISO 18788:2015 or align to our policies and procedures to ensure a complaint and resilient security operations delivery framework.

If you would like to hear how Peregrine Risk Management provides global journey management solutions for our clients, please contact our helpful team on:

Tel: +44 (0) 1531 80 60 00

Email: enquiries@peregrine-rm.com

Web: www.peregrine-rm.com

Peregrine

Risk Management

☎

+44 1568 60 70 00

✉

enquiries@peregrine-rm.com

⌂

www.peregrine-rm.com

Office 7, Thrive Hubs,
Ocean Cresent,
25 The Cresent,
Plymouth, PL1 3AD