AIRPORTS COUNCIL INTERNATIONAL

Landside Security HANDBOOK

First Edition 2018

In collaboration with ARUP

AIRPORTS COUNCIL INTERNATIONAL

Landside Security HANDBOOK

First Edition 2018

Published by: ACI World, Montreal, Canada

ACKNOWLEDGEMENTS

ACI World would like to thank the following contributors and authors of this handbook:

- Members of the ACI World Security Standing Committee (WSSC)
- ACI EUROPE Security Committee for best practices guidance referred to throughout this handbook
- Arup for developing the Building design chapter
- The International Civil Aviation Organization (ICAO) for input on the risk management chapter and landside design
- The International Air Transport Association (IATA), in particular for the material on crisis communications
- Lam-Lah Consulting and BIRDe Technologies LLC for contributions to response and recovery chapters
- Andrew McClumpha, McClumpha Associates for input to the security culture and training sections
- UK Department for Transport for risk assessment methodology, and significant input to the airport design sections
- TH Airport Consulting for input to the measures section
- Centre for the Protection of National Infrastructure (CPNI) for material on security culture. Crown copyright information is reproduced with the permission of the Centre for the Protection of National Infrastructure (CPNI)

DISCLAIMER

The information contained in this publication is subject to constant assessment in the light of changing requirements and regulations. No subscriber or other reader should act on the basis of any such information without referring to applicable laws and regulations and/or without obtaining appropriate professional advice. Although every effort has been made to ensure accuracy, Airports Council International (ACI) World shall not be held responsible for loss or damage caused by errors, omissions, misprints or misinterpretation of the contents hereof. Furthermore, ACI expressly disclaims all and any liability to any person, whether a purchaser of this publication or not, in respect of anything done or omitted, and the consequences of anything done or omitted, by any such person through reliance on the contents of this publication.

No part of the Landside Security Handbook may be reproduced, recast, reformatted or transmitted in any form by any means, electronic or mechanical, including photocopying, recording or use of any information storage and retrieval system, without prior permission from:

Director, Security, Facilitation and Information Technology
Airports Council International - ACI World
800 rue du Square Victoria
Suite 1810, PO Box 302
Montreal, Canada

Landside Security Handbook
First Edition (2018)

Copies of this publication are available from:
Publications Department
Airports Council International - ACI World
800 rue du Square Victoria
Suite 1810, PO Box 302
Montreal, Canada

aci@aci.aero
Web: www.aci.aero

ISBN 978-1-927907-56-6

©2018 Airports Council International. All rights reserved.

FOREWORD

by Angela Gittens, Director General, ACI World

The terrorist attacks in the landside areas of Brussels Airport and Atatürk Airport in Istanbul in 2016, and the shooting in Fort Lauderdale in 2017, brought the security of the public areas of airports sharply into focus again for all aviation stakeholders, governments, the traveling public and in the media. Ensuring the security of the traveling public is a top priority for Airports Council International (ACI) and its member airports, and is a prerequisite for a sustainable worldwide aviation system.

In 2017, a new standard was introduced by ICAO for landside security, as well as some helpful guidance material for States in the ICAO Security Manual. To complement that guidance material, and the guidance developed by ACI EUROPE for airports, ACI World has drawn from best practices and examples globally in order to provide a comprehensive handbook for airports addressing this issue. It covers many different aspects from risk assessment, security culture and training, through to building design and process flows.

We would like to thank members of the ACI World Security Standing Committee for their contributions and to our World Business Partners, ACI EUROPE, the International Civil Air Organization and the International Air Transport Association for enabling us to use and reference their materials. We especially acknowledge Arup which provided detailed input to the terminal design section.

We trust that the handbook will provide a useful guide to the planning for and response to landside incidents in the terminal environment; it provides many examples and options for a variety of operating environments.

Angela Gittens
Director General
ACI World


D

CONTENTS

1 INTRODUCTION

Aviation-specific security regulations focus on the airside spaces (non-public spaces of airports accessible only to air passengers who hold a valid boarding pass and to security cleared staff). These regulations are designed to prevent unlawful interference with air transport. Landside spaces (airport spaces accessible to the general public) are subject to general security regulations enacted by national authorities. It is therefore up to these national authorities to review and coordinate with airports to identify the appropriate measures that match their specific threat scenario.

Various bodies have produced both regulations and guidance covering a number of aspects of airport security, both nationally and internationally, including from within the industry. Examples include the ICAO Aviation Security Manual Doc 8973, ECAC Guidance material and government design guidelines.

This Handbook is intended to complement such material by offering guidance specifically regarding landside security for airports, drawing on the experiences from airports around the world. It may be used as a standalone guide, or may complement an APEX in Security review.

The handbook is intended to help airports benefit from the experiences of others in ensuring that all aspects of prevention, deterrence and incident management have been considered in their own security programmes. It updates and brings together the best elements of managing security from current experience of those involved in this important task from airports around the world.

Understanding that all airports face different threats, have differing models of service delivery and the need for compliance with local regulation, each chapter suggests options and solutions that might be applicable. National regulatory requirements may also dictate measures that must be implemented.

Not all of the measures identified would necessarily be the responsibility of the airport; in many instances airports own the real estate landside but the responsibility for public spaces lies with local law enforcement. However, the measures can be used in discussion with local authorities and national regulators when determining the risk level and appropriate actions. In all cases, measures should be avoided that create new vulnerabilities such as additional queues in public areas.

Elements of landside security

Effective security relies on a multi-layered approach, which brings together a combination of physical measures, detection and deterrence methods and human factors. This handbook covers all elements to provide a comprehensive approach and options in each category. Broadly, it breaks down into the following areas:

In terms of prevention, the ideal scenario is to stop any attack before it reaches the airport environment. The most important layer, therefore, is intelligence. Co-operation and information sharing between agencies, law enforcement and airport authorities must be the top priority. Coupled with this is the need for well-defined responsibilities and accountability for measures between the airport, the regulator and other agencies such as the police and public safety so that vulnerabilities are identified and mitigated to the greatest extent possible and incidents are dealt with swiftly and effectively.

	People	Physical design	Dynamic Measures
Prevention	Threat and intelligence sharing Risk analysis Public awareness Staff training Clear allocation of responsibilities	Building design Roadway design Blast proofing Terminal and flow design	Physical presence of patrols Communication
Detection	Behavior detection, security culture, public awareness and reporting	Well lit areas, good terminal design	Monitoring, CCTV, patrols, overt and covert screening, canines
Response and recovery	Crisis management processes, training, communication	Evacuation routes, design to limit impacts	Communication processes, evacuation procedures, business continuity and contingency plans

2 RESPONSIBILITIES

2.1 Regulatory framework

The International Civil Aviation Organization (ICAO), a specialized agency of the United Nations, establishes and maintains international Standards and Recommended Practices (SARPs), which are fundamental tenets of the Convention on International Civil Aviation (the Chicago Convention).

SARPs are critical to ICAO Member States and other stakeholders, given that they provide the fundamental basis for harmonized global aviation safety and efficiency in the air and on the ground.

Annex 17 of the Chicago Convention defines SARPS relating to aviation security and lays down a requirement for each state to establish and implement a written national civil aviation security program (NCASP) to safeguard civil-aviation operations against acts of unlawful interference, through regulations, practices and procedures which take into account the safety, regularity and efficiency of flights.

Following the landside incidents in Brussels and Istanbul (see Chapter 3), a new standard was developed for Annex 17 of the Chicago Convention, requiring ICAO Member States to:

- Ensure that landside areas are identified;
- Ensure that measures are established to mitigate the risk and deter possible attacks; and
- Coordinate measures between departments and agencies and identify appropriate responsibilities in the national civil aviation security program (NCASP).

2.2 National agreement

Many States will have already defined risks to landside areas and will have included measures in their respective NCASPs. However, the introduction of the new standard may have required some modification to national regulations, or in some cases the introduction of completely new measures.

Airports should review their national regulations and ensure that they meet the obligations set out for landside security. These might include many of the aspects considered in this handbook, such as building and road design, crisis planning, risk and vulnerability assessment and a range of measures such as screening, checking, patrolling and detecting suspicious behaviour.

2.3 Definition of "landside"

ICAO defines "landside" as "Those parts of an airport, adjacent terrain and buildings or portions thereof that are not airside, as identified by States and relevant entities in their security programs."

However, for the purposes of defining which measures need to be implemented, a more useful definition could be based on the threat and risk environment. For example, this might include terminal areas where there are mass gatherings of people, but it might exclude distant car parks.

Targets may include:

- The public, airport staff and specific operations (e.g. a specific aircraft operator's check-in counter) in a landside area;
- Terminal buildings, or part thereof, the loss of which would have significant impact on the functioning of the airport and the local or even the national economy;
- Critical infrastructures such as air traffic control facilities and fuel farms; and
- Interdependent infrastructure, such as public transport services (bus and rail).

Each airport must make its own risk assessment for each area, in cooperation with its appropriate authority. A clear definition of the risk will be critical to defining the scope of measures and ensuring that the focus of the measures required is on genuinely high-risk areas—not on all property owned by the airport.

It is recommended that "landside areas" are clearly defined on an airport plan and agreed with the national regulator or the appropriate authority.

2.4 Agreement on responsibilities

Addressing the security of landside areas of airports within aviation-security regulatory frameworks can be

challenging, since what constitutes landside areas differs considerably from airport to airport and security arrangements for them may involve multiple authorities and entities.

Considering the targets above and the possible attack scenarios, the responsibility for each measure in each area must be clearly defined. For example, an airport might be responsible for patrolling the perimeter of the airport, but a local law-enforcement agency may be responsible for surveillance and patrol of associated public infrastructure such as a train station.

Some or all of the following parties may have some responsibility for security:

- Appropriate authority for aviation security;
- Airport operator;
- Airport security manager;
- Airport-security service providers;
- Law-enforcement authority;
- National armed forces;
- Emergency-response units and/or first responders;
- Other government agencies;
- Aircraft operators;
- Airport tenants;
- Municipal authorities;
- Border-control authorities such as customs and immigration agencies;
- General aviation agencies;
- Regulated agents;
- Handling agents; and
- Air navigation service providers.

2.5 Agreement on measures

Measures for risk mitigation and threat response probably will be defined to a certain degree in the NCASP. However, the details of implementation may vary from airport to airport. So discussions should be conducted to determine which measures are most appropriate to the risk environment, under normal operating circumstances; what measures should be implemented in a heightened threat situation; and who is responsible for each. (See Chapter 3, 'Threat and Risk', for further details regarding possible measures.) During discussions on landside definition, measures and responsibilities, it will be helpful to engage the airport security committee. This might include representatives from police, the port authority, border-control agencies, aircraft operators, security service providers, local public transport operators and retail representatives.

For each measure, agreement should be made as to who is responsible for human resources, technology, implementation and cost.

Once measures have been agreed, they should be clearly defined in the Airport Security Program (ASP). For each airport area, clearly define responsibilities and measures and document them on airport plans. It is also important to identify areas to be excluded from measures.

2.6 Information sharing

Timely sharing of relevant threat information between government agencies and the airport authority will be important to provide input to the ongoing evaluation of measures and any decisions regarding the elevation of the threat level.

A mechanism should be agreed to share threat information among local law-enforcement agencies, intelligence agencies and security-cleared airport staff. The airport security manager should review which staff members have security clearances and ensure that sufficient resources are in place to cover absences, and inform authorities of the points of contact.

Equally, credible threat information received by the airport authority or its security team should be shared with local law-enforcement agencies and the appropriate authority.

Channels of communication for specific threat information should be defined, including responsibilities for implementing a response. A contact list should be created and maintained for parties both at the airport and at relevant agencies.

3 THREAT AND RISK

All threats, landside or otherwise, are most effectively managed by identifying, understanding and addressing the potential risks. The identification and prioritization of risks enables airports and regulators to determine and implement proportionate measures and controls to mitigate each type of risk.

3.1 Understanding threats

3.1.1 Actors and motivation

Public spaces are terrorist targets for a variety of motives, and aviation is a high-profile target. Despite enhancements to the security system both in public areas generally and as part of aviation security, terrorists continue to develop new techniques and weapons in hope of circumventing security measures. In general, target assessments show that in selecting a target for attack, terrorists, whether from an organized group or as radicalized individuals, aim to achieve any of the following objectives:

- Inflicting mass casualties;
- Causing economic disruption;
- Making a symbolic statement; and
- Generating public anxiety.

Terrorists have varied cultural and social backgrounds, live in differing social circumstances and act from a variety of different extreme motivations and intentions in committing or planning acts of terrorism. They may act for political, religious, social, environmental and/or personal (e.g. economic or mental health) reasons. Types of terrorists may include:

- Members of established and organized international terrorist groups;
- Members of regional affiliates and allies of such groups;
- So-called 'home-grown' terrorists, or radicalized individuals who have limited or no links to such groups; and
- Radicalized individuals who travel to areas of conflict and undergo training and militarization to then plan and execute attacks outside the conflict zone.

In conducting a risk assessment, it is necessary to assemble information about the threat, particularly its possible targets and the modus operandi likely to be used. Such information may come from a variety of sources, including:

- Actual incidents, including successful or thwarted attacks on aviation, which provide information on terrorist objectives and methodologies;
- Closed sources, primarily counter-terrorist intelligence and assessments, which may be gathered or generated by intelligence, law enforcement and other agencies of States; and
- Open sources, which may include publicly available information on unusual or suspicious occurrences and the availability of items that could be used for terrorist purposes, and any other information that may contribute to the threat picture.

3.1.2 Examples of previous incidents[1]

Fort Lauderdale, Florida, United States, January 2017

A mass shooting occurred at Fort Lauderdale–Hollywood International Airport in Broward County, Florida, United States, on January 6, 2017, near the baggage claim in Terminal 2. Five people were killed and six others were injured in the shooting. Some 36 people sustained injuries in the ensuing panic.

The shooter opened fire with a semi-automatic pistol in the airport at about 12:53 EST, in the baggage claim area of Terminal 2. Video showed travelers rushing out of the airport and hundreds of people waiting on the tarmac as numerous law enforcement officers rushed to the scene. Part of the panic occurred following "unfounded reports of additional gunshots"; the false alarm touched off a panic in other terminals.

The shooting lasted 70 to 80 seconds. The suspect lay down on the ground after he stopped shooting, having run out of ammunition. Broward County Sheriff Scott Israel stated that law enforcement officers did not fire shots and that the gunman was arrested without incident. The suspect flew from Anchorage,

[1] Accounts of the incidents in this section have been retrieved from Wikipedia, 29 September,2017 and are based on public news reports.

connecting through Minneapolis–Saint Paul International Airport. Investigators say that he checked a declared 9mm pistol in his baggage before retrieving it in Fort Lauderdale and loading the gun in the airport bathroom just before the attack.

Atatürk Airport, Istanbul, Turkey, June 2016

A terrorist attack, consisting of shootings and suicide bombings, occurred on 28 June 2016 at Atatürk Airport in Istanbul, Turkey.

Gunmen armed with automatic weapons and explosive belts staged a simultaneous attack at the international terminal of Terminal 2. Forty-five people were killed in addition to the three attackers, and more than 230 people were injured.

Shortly before 22:00 Istanbul time, two assailants approached the x-ray scanner at a security checkpoint, and opened fire. A security camera video showed that one of the bombers was about 24 metres inside the international terminal when he detonated his suicide bomb. According to Turkish officials, one of the explosions was set off by a third attacker in the parking lot across the street from the terminal. A closed-circuit television (CCTV) video of this incident showed an armed assailant walking and firing at people inside the terminal. The gunman was then shot by a security officer and fell to the ground, following which the security officer approached the gunman to investigate. The suicide belt then detonated.

During and immediately after the attacks, hundreds of passengers and people inside the airport hid anywhere they could in shops, washrooms, and under benches.

Turkish officials said the attackers were acting on behalf of the Islamic State of Iraq and Levant and had come to Turkey from ISIL-controlled Syria. No-one claimed responsibility for the attack.

Brussels Airport, Belgium, March 2016

On the morning of 22 March 2016, three coordinated suicide bombings occurred in Belgium: two at Brussels Airport in Zaventem and one at Maalbeek metro station in central Brussels. Thirty-two civilians and three perpetrators were killed, and more than 300 people were injured. Another bomb was found during a search of the airport. Islamic State of Iraq and the Levant (ISIL) claimed responsibility for the attacks.

Two suicide bombers, carrying explosives in large suitcases, attacked a departure hall at Brussels Airport in Zaventem. The first explosion occurred at 07:58 local time in check-in row 11; the second explosion occurred about nine seconds later in check-in row 2. The suicide bombers were visible in CCTV footage.

A third suicide bomber was prevented from detonating his own bomb by the force of a previous explosion. The third bomb was found in a search of the airport and was later destroyed by a controlled explosion. Belgium's federal prosecutor confirmed that the suicide bombers had detonated nail bombs.

Domodedovo International Airport, Moscow, Russia, January 2011

A suicide bombing took place in the international arrival hall of Moscow's Domodedovo International, in Domodedovsky District, Moscow Oblast, on 24 January 2011.

The bombing killed 37 people and injured 173 others, including 86 who had to be hospitalized. Russia's Federal Investigative Committee later identified the suicide bomber as a 20-year-old from the North Caucasus, and said that the attack was aimed "first and foremost" at foreign citizens.

The explosion affected the baggage-claim area of the airport's international arrivals hall. Some reports have suggested that the explosion was the work of a suicide bomber. Investigators said the explosion was caused by an "improvised device packed with shrapnel, pieces of chopped wire" and an explosive material equivalent in force to between two and five kilograms of TNT.

According to Russian newspaper accounts, the bombing was carried out by two suicide bombers, a man and a woman. Another three accomplices who had kept their distance from the blast were sought, but the source of the attack remained unclear.

Glasgow Airport, United Kingdom, June 2007

The 2007 Glasgow Airport attack was a terrorist ramming attack which occurred on 30 June 2007 at 15:11 local time when a Jeep Cherokee loaded with propane canisters was driven at the glass doors of the Glasgow Airport terminal and set ablaze. Although the doors were damaged, security bollards outside the entrance stopped the car from entering the terminal, inside which there were 4,000 people. Thus the incident provided potential for many fatalities.

The driver of the car was burned severely in the ensuing fire and five members of the public were injured, none seriously. Some injuries were sustained by those assisting the police in detaining the car's occupants.

The vehicle was reported to have several petrol containers and propane gas canisters on board. When the Jeep failed to explode, one man threw petrol bombs from the passenger seat and the other doused himself in petrol and set it alight. Police indicated the vehicle burst into flames when it was driven at the terminal.

3.2 Risk assessment

3.2.1 Risk-assessment methodology[2]

Risk can be defined as: "The probability of an act of unlawful interference being successfully carried out on a specific target, based on an assessment of threat, vulnerability, and consequence." Assessing risk formally can enable an airport to prioritize the mitigation measures put in place, in agreement with its national regulator and local security forces.

This section provides an example methodology for a risk assessment. There are many variations and airports can use their preferred methodology as appropriate and in line with that used by their regulator.

The risk-assessment process comprises three elements:

a) Analysis of plausible threat scenarios and their likelihoods, and consequences;
b) Residual risk assessment, taking account of vulnerability and current mitigations; and
c) Recommendations for further possible measures.

The key components for completion of the risk assessment are:

a) *Threat scenario*—Identification and description of a credible attack comprising a target—in this case an area of the airport terminal—and the means and methods of the attack (such as an improvised explosive device, a vehicle-borne explosive device or an automatic weapon);

b) *Threat/likelihood of an attack*—The probability or likelihood of that attack being attempted, based on terrorist intentions and capabilities but NOT taking into account current security measures;

c) *Consequences*—The nature and scale of the consequences of a specific attack, in human, economic, political, and reputational terms under a reasonable worst-case scenario;

d) *Current mitigating measures*—Assuming no threat can be eliminated entirely, measures already in place to prevent or reduce the impact of the scenario. These may be physical (for example vehicle-proof bollards), procedural (such as random checks of visitors), or involve personnel (such as staff training and behavior detection);

e) *Vulnerability*—The extent of the remaining vulnerabilities once the current mitigating measures have been taken into account; and

f) *Risk*—The overall risk that remains, assuming current mitigating measures have been implemented, taking account of threat likelihood and consequences.

The resulting risk assessment may lead to recommendations for possible additional mitigation—measures that the airport may implement to further mitigate residual risks where necessary, either under normal operating circumstances or at times of heightened threat level. Our aim is not to eliminate risk, only to manage it to an acceptable level.

[2] The risk-assessment methodology used here is largely drawn from the ICAO methodology. This section provides an overview, but further details can be obtained from ACI or ICAO; a detailed Risk Management Workshop is also available.

3.2.2 Possible threat scenarios

Threat scenarios will be different for each airport, but should be specific in terms of target, adversary and method of attack. For example "bomb in the airport building" cannot be assessed, but "vehicle-borne improvised explosive device parked outside terminal" can be. Each threat scenario should only assess one single attack method, and the list should be as comprehensive and specific as possible. Scenarios should be developed for each area of the facility, especially if security measures vary from terminal to terminal.

Threat scenario	**Methodology** (description of methods)	
Person-borne IED on body detonated at check-in area	**Target/Asset:** **Adversary:** **Modus operandi:**	Check-in queue Airport visitor IED on the body, suicide attack
IED in bag carried by attacker detonated at check-in area	**Target/Asset:** **Adversary:** **Modus perandi:**	Check-in queue Airport visitor / passenger IED in baggage
Armed assault from gallery overlooking ticketing desks	**Target/Asset:** **Adversary:** **Modus operandi:**	Ticketing queue Airport visitor Automatic weapon
Vehicle-borne IED detonated in front of terminal building	**Target/Asset:** **Adversary:** **Modus operandi:**	Terminal entrance infrastructure and visitors entering terminal Public Vehicle-borne IED

These scenarios are by no means exhaustive and need to be developed by each airport for its own particular environment and operation, in cooperation with its regulator and local law-enforcement agencies.

THREAT AND RISK

For each scenario, it is also useful to define responsibilities; an example from Brussels Airport is provided below.

Attack scenario	Responsibility	Stakeholders
1. **Terrorists using a vehicle to enact a penetrative attack.** A vehicle has bypassed the security implemented on the approach to BAC and has access to the airport site. This vehicle then is able to enact a penetrative attack (ramming) of a critical asset such as that targeted at Glasgow Airport in 2007. This may be a pre-cursor to a vehicle-borne IED (VBIED), or as a method of entry for follow-on attacks. **Risk to life.**	BAC/FedPol	• BAC • FedPol • Military • Security provider
2. **Terrorists using a vehicle-borne IED (VBIED).** A vehicle carrying an explosive device has bypassed the security measures in place. It is then detonated on the airport site, at the threshold, or inside a critical asset. **Risk to life.**	BAC/FedPol	• BAC • FedPol • Military • Security provider
3. **Terrorists on foot using small arms or manual weapons.** A terrorist has gained access to the airport site, either on foot or via taxi, car or public transport. The terrorist then conducts attacks on passengers within the airport site at the threshold or inside critical assets. **Risk to life.**	BAC/FedPol	• BAC • FedPol • Military • Security provider
4. **Terrorists on foot detonating a person-borne IED (PBIED).** A terrorist has gained access to the airport site, either on foot, via a taxi, car or public transport. The terrorist then detonates the PBIED within the airport site at the threshold or inside a critical asset. **Risk to life.**	BAC/FedPol	• BAC • FedPol • Military • Security provider
5. **Insider threat** A BAC employee uses his or her access either to enable the other scenarios above or to conduct them personally. **Risk to life.**	BAC/FedPol	• BAC • FedPol • Military • Security provider

3.2.3 Threat assessment (likelihood)

The threat assessment should take into account the intent (the perpetrator's motivation and objectives) and the capability (whether the threat scenario is practical from a training and materials perspective). It might also consider whether such a scenario has been attempted previously. Information is available both from open sources and by working with local regulators, intelligence agencies and law-enforcement agencies. Threat is usually ranked on a scale of 1 to 5, from low (theoretically plausible but no examples or apparent capability) to high (very plausible, with strong evidence of capability, intent and planning).

3.2.4 Consequences

The consequences assessment looks at the reasonable worst-case consequences of an attack scenario, including human, psychological, reputational, disruptive and economic factors.

As with threat, consequences are given a ranking from low (very little impact in terms of possible casualties or disruption) to high (mass casualties and inability to operate).

3.2.5 Vulnerability

When assessing vulnerability, it is important to consider the target and the characteristics for each scenario. All relevant mitigation should be taken into account, including physical, procedural and personnel measures. These might include factors that take place at booking time, or before arrival at the airport (such as risk assessment and intelligence), through to physical measures implemented in the terminal building. Not all measures may be implemented by the airport itself, so it is important to consult with local law-enforcement and civil aviation authorities.

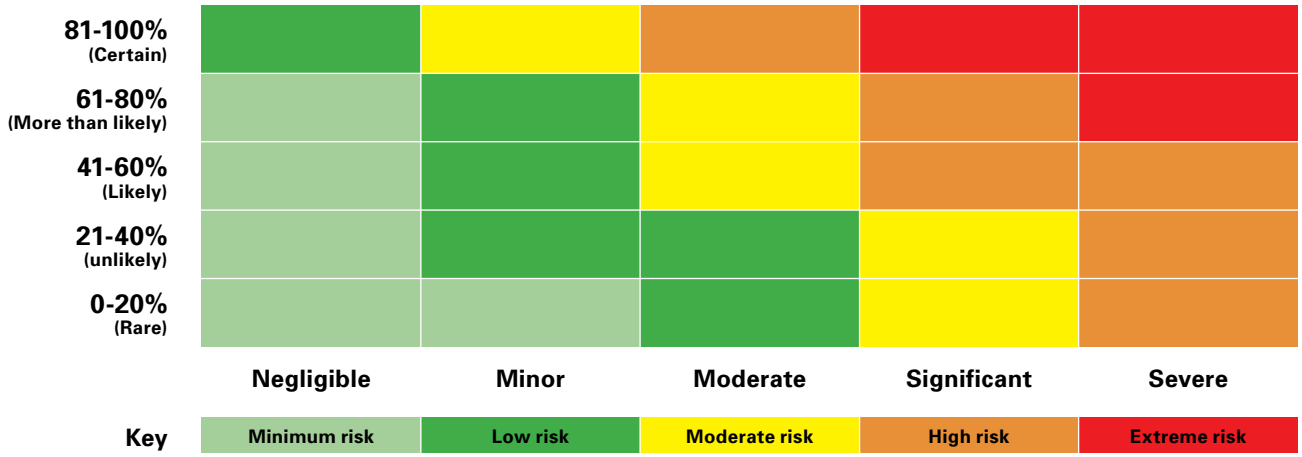
Whatever has not been mitigated is the remaining vulnerability, which can again be ranked on a scale of low (mitigating measures generally regarded as effective are in place and well implemented) to high (no mitigation is in place or available).

The process of identifying vulnerabilities should be regarded as a means for improvement and a constructive exercise. It is imperative that the risk assessment is kept confidential and only shared with those who need to know and it should not be used to expose weaknesses or failures by the airport or staff. Only by identifying possible vulnerabilities can improvements be made.

3.2.6 Risk register/matrix

The threat, consequence and vulnerability or each scenario can be recorded in a risk matrix, to help determine the risk score. Risk scores can then be derived from a combination of threat, consequence and vulnerability.

Using the threat scenario examples from above, the resulting matrix might be:



Using the threat scenario examples from above, the resulting matrix might be:

Threat scenario	Threat (likelihood)	Consequence	Vulnerability	Risk Score
Person-borne IED on body detonated at check-in area	HIGH	HIGH	MED-HIGH	HIGH
IED in bag carried by attacker detonated at check-in area	HIGH	HIGH	MED	HIGH
Armed assault from gallery overlooking ticketing desks	MED-HIGH	MED-LOW	LOW	MED-LOW
Vehicle-borne IED detonated in front of terminal building	HIGH	MED-HIGH	LOW	MED

Note: this is only an example and the risk matrix will vary from airport to airport. Some risk-assessment methodologies assign a score to each category in order to identify a numerical result for risk, but some use ranges of different scores.

3.2.7 Measures in normal threat environment

From the resulting risk score, the airport, in cooperation with the regulatory authority and local law-enforcement agencies, can determine which risks need to be addressed.

Decisions may include:

- Whether further research on a risk-assessment component is necessary;
- Whether a risk needs mitigation;
- The priorities for mitigation;
- Whether an activity/operation should be undertaken; and
- Which of a number of mitigation options should be followed.

Risk scores	
High	May require immediate action in the form of specific countermeasures
Medium-high	May require implementation of specific countermeasures
Medium/Moderate	May require implementation of specific countermeasures—on a case-by-case basis and depending on threat level
Medium-low/Minor	May require the implementation of specific countermeasures that may enhance security and reduce probability of the occurrence
Low/Negligible	Typically does not require the implementation of specific countermeasures, unless operating in a heightened-threat environment or on specific occasions

Understanding *why* a vulnerability exists is the key to developing effective mitigation recommendations. This might include lack of knowledge ("I don't know what to do"), lack of resources or infrastructure, or lack of clarity on responsibilities.

3.2.8 Operating in a heightened security environment

When threat levels are increased, it may be necessary to have additional measures in place that can be rolled out at very short notice. These measures would typically be of the type that can be easily flexed to respond to changing events, such as an increase in random checks/screening or increased patrolling and surveillance.

The airport, the regulator and local law enforcement should agree a) who is responsible for delivering additional measures; and b) what circumstances trigger the additional measures to be implemented. Equally, pre-defined criteria should be set for returning to normal operations so that enhanced measures

do not become the normal operation, unless a risk assessment indicates this is necessary. The criteria may be time- or intelligence-driven. For example, increased measures may be put in place for 7 days following a specific threat and can be removed provided that no further intelligence indicates the threat is still imminent.

3.3 Mitigation options

It is recommended that when exploring risk-reduction options, measures other than those that are security-centric are considered, because there are ways in which risk can be reduced besides the application of security-centric measures. This is achieved by understanding and addressing the root cause(s) of the risk—e.g. why the target is attractive, why the vulnerability exists, etc. Addressing the root cause of the risk can be achieved by non-security measures.

The following example illustrates this principle:

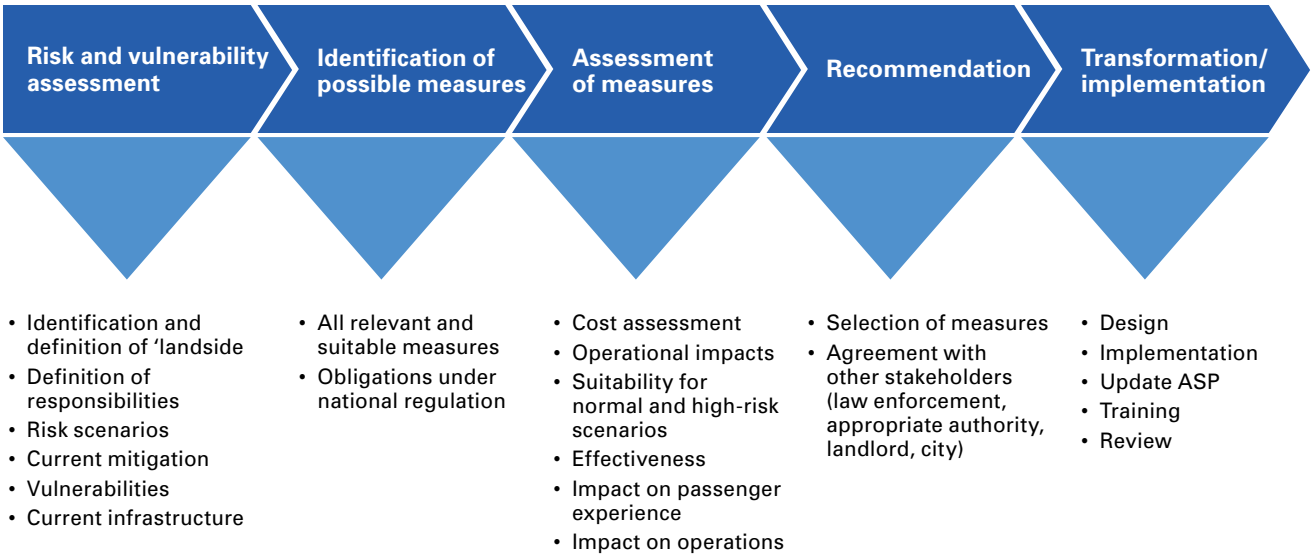
The check in area is an attractive target. Why? Because it is crowded. Rather than overlaying security measures, can the risk be reduced by reducing the attractiveness, i.e. reducing the risk? The measure may be to change the check-in layout, work with airlines to increase online check-in, or consider using off-site check-in or bag-drop facilities. None of these measures are security-specific, yet they all reduce the risk of attack by addressing the underlying cause of the risk—crowding. These measures also provide additional passenger-experience advantages.

The business case associated with the application of measures that are not explicitly security measures can be stronger than for a security-centric measure. This is because they often address other business objectives such as improved passenger experience, reduced operating and capital costs, and improved lifespan of assets and infrastructure. In some cases, they can even be revenue-generating. This further supports the other principles associated with the application of mitigation measures that aren't necessarily directly associated with risk reduction, namely that such measures should have minimal interference with facilitation. As noted above, in some cases improved facilitation provides improved security outcomes.

4 MEASURES AND TECHNOLOGIES

Measures will probably be defined to a certain degree in the National Civil Aviation Security Program (NCASP). However, the details of implementation may vary from airport to airport, so discussions should be conducted to determine which measures are most appropriate to the risk environment under normal operating circumstances; what measures should be implemented in a heightened threat situation; and who is responsible for each.

There is a range of options available to airports, depending on their operational realities and their risk environments.



Once measures have been agreed, they should be clearly defined in the Airport Security Program (ASP). For each airport area, the airport should define responsibilities and measures clearly and document them on airport plans. It is also important to identify areas to be excluded.

4.1 Measures for deterrence and prevention[3]

4.1.1 Patrols

One of the more effective methods used in preventing and deterring landside attacks is to perform patrols around the airport environment. The patrols should be undertaken in order to monitor:

- The boundaries between landside, airside, security restricted areas, and, where applicable, demarcated areas; and
- Areas of the terminal, and in proximity to the terminal, that are accessible to the public, including parking areas and roadways.

Patrols can be effective as a visible deterrent, for searching and finding unaccompanied baggage and other items and as a method for detecting suspicious behaviour.

The frequency and means of undertaking surveillance and patrols should be based on a risk assessment, should take into account the need for unpredictability and should be approved by the appropriate authority.

[3] With thanks to ACI Europe Aviation Security Committee and TH Consulting for guidance material used in this chapter.

They should take into account:

- The size of the airport, including the number and nature of its operations;
- The layout of the airport, the topography of the surrounding area outside the perimeter fence and in particular the interrelationship between the areas established at the airport; and
- The possibilities for and limitations of means of performing surveillance and patrols.

The parts of the risk assessment relating to the frequency and means of undertaking surveillance and patrols should, upon request, be made available in writing for compliance-monitoring purposes.

Foot patrols

Foot patrols should take place in all relevant landside areas. Officers can be in uniform (increasing the deterrent effect) and covert—dressed in plain clothes (posing as airport workers or passengers/visitors).

The relevant areas need to be defined and identified by the local risk assessment. The following areas need to be considered:

- Terminals;
- Access points to the terminal;
- Check-in counters and areas;
- Arrival halls;
- Queuing lanes;
- Access points/checkpoints to airside; and
- Areas identified by MANPADS assessment and other vulnerable areas.

Patrols should be carried out according to national and local requirements, by:

- Airport security staff (or contracted security service providers); and
- Law enforcement officers.

Vehicle patrols

There should be vehicle patrols in all relevant landside areas. The relevant areas need to be defined and identified by the local risk assessment. The following areas need to be considered:

- Outer perimeters of terminals;
- Checkpoints to the security restricted area/airside;
- Heightened points at the outer perimeter; and
- Areas identified by MANPADs assessment and other vulnerable areas.

High-visibility patrols of law-enforcement and security staff, including canine teams, may not only act as a deterrent but may also provide rapid emergency response. Such patrols may conduct random checks, while covert behaviour detection officers (BDO) may identify suspicious behaviour patterns.

4.1.2 Explosive Detection Dogs (EDD)

Explosive detection dogs provide a useful explosive-detection capability as well as a strong deterrent effect. Dogs used specifically for explosive protection (not for general patrol) should be trained to detect only explosives, not narcotics. Nor should they be used as protection dogs.

Explosive detection dogs may be deployed using a free-running method, where the handler commands the dog to perform specific tasks in a controlled manner or on a lead, to sample directly items such as bags.

Explosive detection handler-dog teams must be specially trained, approved by the appropriate authority or law enforcement and submitted to quality control for the purpose of explosive detection for aviation security.

In general, this method should be complementary to other detection methods. There are many benefits to using explosive detection dogs, such as excellent detection capability, portability and deterrent effect. However, it should be recognized that dogs can only work for limited periods without rest and require special training, handling and facilities. In many cases, canine teams are deployed by law enforcement agencies rather than the airport.

Explosive detection canine – Courtesy of Adelaide Airport

Explosive detection dog teams can be complementary to behavior detection officer teams, at screening points or deployed for random checks.

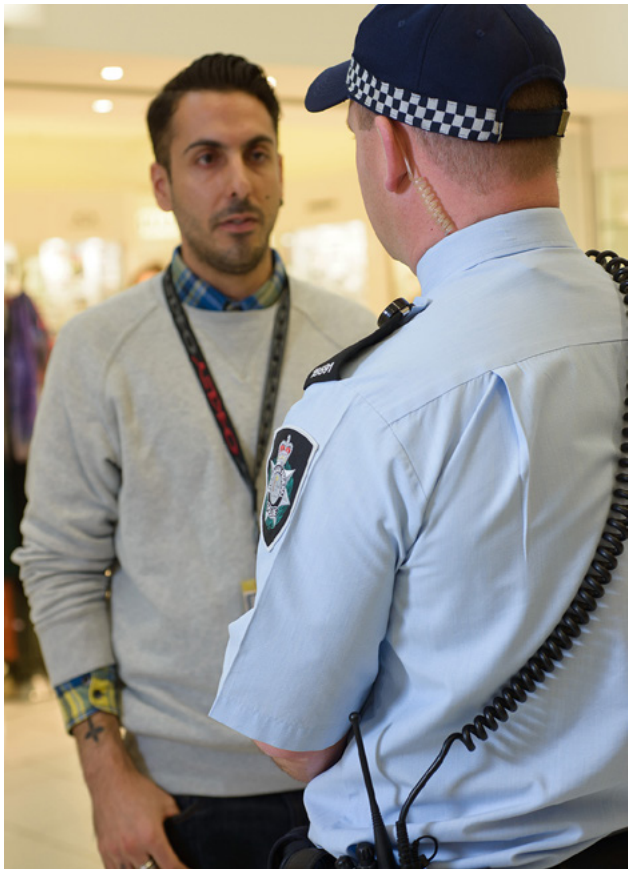
4.1.3 Remote and stand-off screening

In a heightened threat environment, it may be necessary to establish additional screening before people enter the airport terminal. Any such screening activities should avoid creating new vulnerabilities such as queues and crowds inside or outside terminal buildings. It may be appropriate to use random or targeted checks. Mobile technologies or techniques such Explosive Trace Detection (ETD), behaviour detection officers (BDO) or explosive detection dogs (EDD) may be appropriate to screen passengers quickly and efficiently.

4.1.4 Behaviour detection

Behaviour detection personnel can be used as both a method of detection and as a deterrent. It should be noted that the analysis of behaviour is not a perfect science and opinions differ with regard to its effectiveness. However, reviews of existing behaviour-detection programs show that selecting persons for additional security controls on the basis of suspicious behaviour has been effective in identifying those involved in criminal activity.

Behaviour-detection techniques need to differentiate between behaviour characteristics inherent in the airport environment and actual suspicious behaviours. For example, stress caused by delays, flight cancellations or fear of flying may cause some



Behaviour detection module

passengers to appear anxious. Some indicators of suspicious behaviour are listed below which may be useful for staff training, but specialized behaviour detection officers should receive professional training in behaviour-detection and questioning techniques.

The location of behaviour detection officers will vary depending on the airport environment. In the example above, officers are stationed in special areas at the terminal entrance doors and perform random analysis and questioning. Officers may also roam the terminal area or focus on particular processes.

Good interpersonal skills, giving officers the ability to engage strangers in casual but targeted conversations, are a key requirement. Given the sensitivity of the program, consideration should also be given to the level of security clearance to be held by behaviour detection officers.

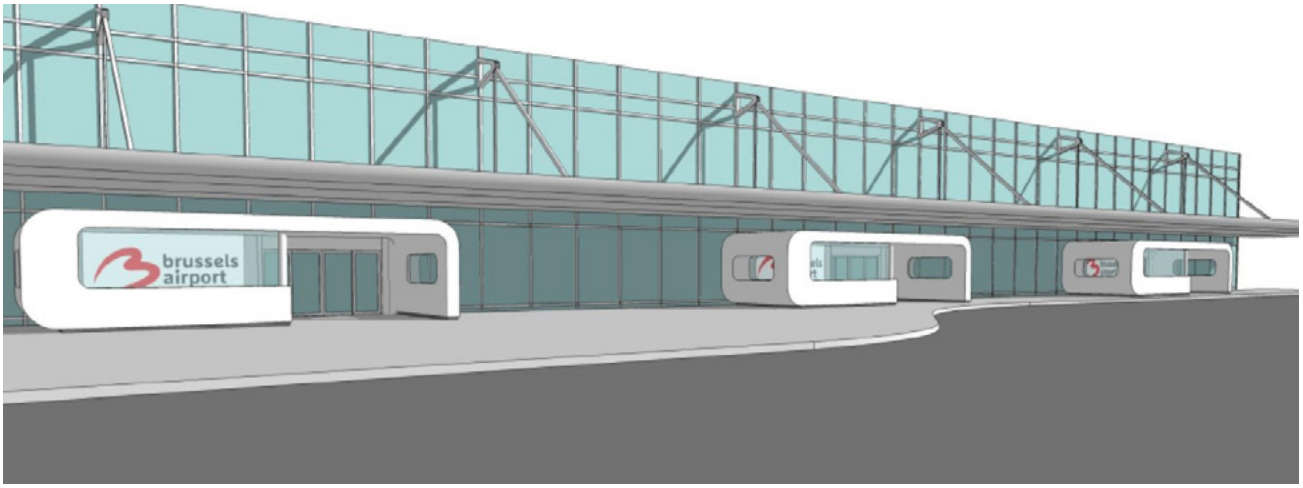
The following list suggests possible indicators of suspicious behaviour which could lead to further investigation that might identify or pre-empt a possible threat to an area and alert the need for an appropriate response. This list is indicative and should not be considered exhaustive:

- Displaying an unusual interest in airport operations and security measures, such as:
  - Making enquiries about procedures
  - Measuring distances
  - Repeatedly visiting particular locations
  - Taking excessive photographs (especially of items of little artistic value) or making sketches
  - Making notes about operations, timing of shift changes, etc.
  - Closely watching staff and their reactions;
- Wearing unusual clothing, bulky padding or clothing inappropriate to the weather;
- Hiding identity from surveillance cameras;
- Displaying reluctance to show travel documents or presenting suspect documents when asked;
- Displaying anxious behaviour, such as fidgeting, clock-watching and scanning of the area;
- Giving responses that appear rehearsed or do not make sense when questioned;
- Having excessive luggage, especially if the amount is inappropriate for the trip; and
- Having hold baggage but no hand baggage.

4.1.5 CCTV

CCTV is an important surveillance tool that, if correctly managed and monitored, can identify or pre-empt a possible threat to an area and alert the need for an appropriate response.

Many airports use low-definition CCTV in the public area of terminals for flow- and crowd-control purposes. Installation of high-definition cameras monitored from a security control centre may help to identify possible suspicious behaviour as a preventative measure and as an aid to post-incident forensic work. Unless all areas are monitored continuously, CCTV is likely to have limited detection capability. However, it



Behaviour detection infrastructure – Courtesy of Brussels Airport

may have good deterrence value, when used as a layer of a broader security regime.

Planning of CCTV coverage should be a coordinated effort involving all the security stakeholders at the airport and should take account of the risks and vulnerabilities. CCTV installation or upgrade should be coupled with a review of security lighting to ensure that all areas are well lit. Areas that could be considered for monitoring include:

- All vehicles entering the airport and covering all restricted and unrestricted routes;
- The pedestrian area and terminal entrance/exits, sufficient to:
  - Highlight suspicious behaviour by live monitoring
  - Provide retrospective ID coverage of everyone entering/exiting;
- Movement of persons through the terminal, including walkways, ticketing and bag drop areas;
- Passenger screening checkpoints; and
- Any areas that are not within direct line of sight for staff.

In addition to meeting security objectives, CCTV coverage of passenger-screening checkpoints may facilitate the operational analysis of passenger throughput and possible enhancements—in particular, adjustments to staffing levels to reduce the lengths of queues.

CCTV may be operated continually, or can 'cut in' to view a specific area on receipt of an alarm. This enables an operator at a control desk to verify the cause of the alarm and take specific action. Consideration should be given to providing both fixed cameras and movable cameras and whether they should be overt or covert.

Correctly deployed CCTV is also very useful as a post-analysis tool. Particular care should be taken to ensure recorded images are of sufficient quality and that bulk retrieval of stored images is possible without detriment to the system's operation.

4.1.6 Video analytics

To complement CCTV, advanced intelligent video-analytics systems are an emerging technology that can assist in identifying unattended bags and abnormal behaviour outside of normal passenger flows. Functionality such as motion detection, tracking and counting are now available as commercial off-the-shelf products.

Planners should consider whether intelligent video-analytics software can support operators in the control room by creating an alarm if certain behaviours are detected, such as unusual speed, direction of movement or unusual time spent in an area. Using suspect-tracking technology, it is also possible to

track an identified subject's movements easily: where the subject came from, and when, where, and how he/she moved.

Video analytics can be implemented on CCTV systems, either distributed individually on each camera or centralized in dedicated processing systems. Independent video-management software manufacturers are constantly expanding the range of video analytics modules available.

4.1.7 Lighting

Security lighting is essential and its provision and installation should be taken into account at the planning stage. It should provide illumination of all critical operational areas to enable effective patrols and surveillance. Planning and operations should take into account any surveillance systems that may be deployed, such as Closed Circuit Television (CCTV), Number Plate Recognition (NPR) and Intruder Detection Systems (IDS). This will allow the correct lighting type and luminosity to be selected.

4.1.8 Emergency alerting system (blue boxes)

Around the airport property, there are areas such as large parking structures that are not easily accessible in a short time frame when responding to any events. For these larger structures, accessibility to emergency communication is essential for any response. An integrated emergency alerting system is a useful piece of infrastructure that should be in place in such areas so that people have a direct response to the appropriate authority for providing assistance.

The emergency alerting system should be both audible and visible within the area it is installed, so that detection by responding officers can be easily identified. When a unit is activated, the communication link should be with the airport operations control centre, which will coordinate the appropriate response.

4.1.9 Explosive Trace Detection (ETD)

One of the more common methods of explosive detection is the use of portable equipment able to detect explosives of small magnitude. The detection

An airport security screening officer on the job inspecting a luggage using an Explosive Trace Detection wand

is accomplished by sampling non-visible "trace" amounts of particulates. ETD is most commonly deployed at central screening checkpoints as a secondary or random measure, or at boarding gates.

Several types of machines have been developed to detect trace signatures for various explosive materials. The most common technology for this application is ion mobility spectrometry (IMS), which involves 'swabbing' either individuals or baggage for very minute traces of explosive material. IMS units can be transported with ease throughout different areas of the airport and do not require a large amount of space to conduct tests. This makes ETD possible at landside locations, such as at screening points in a high-threat situation.

Other, more portable, handheld solutions for non-invasive imaging and trace detection are becoming available and may offer future solutions with less operational impact.

4.1.10 Staff awareness

Basic security awareness and the ability to recognize suspicious behaviour make non-security staff a valuable asset in the landside environment. All staff and contractors in the airport should receive security training, even if they do not have airside or restricted area access; and simple, immediate reporting mechanisms should be put in place to enable any observed behaviours to be reported to specialized staff quickly. Further information is provided in the 'Security Culture' chapter of this handbook.

4.1.11 Public awareness

Passengers and non-travellers can also provide a valuable resource to supplement more official measures. Airports should issue or publicize instructions to the general public about the importance of notifying any suspicious activities and items to local authorities. For example, displaying posters and/or making public announcements may help raise awareness among both passengers and non-passengers, and further assist in the detection of suspicious activities and unattended items in landside areas of airports. Further information and examples are provided in the 'Security Culture' chapter of this handbook.

4.1.12 Advanced communication techniques

The use of messaging to inform staff and passengers about security issues can additionally send an effective message about the (high) level of security at an airport, without alarming passengers. Posters in terminals might include messages such as:

- "Undercover patrols are in use in the terminal";
- "CCTV is working: if you can see this, we can see you"; and
- "This airport implements security measures that are both seen and unseen."

4.2 Passenger perception

When implementing measures for landside security, consideration should be given as to how measures may be perceived by airport users, and how such measures could impact airport users' experience of using terminal facilities.

A balance needs to be struck between providing enough security information and visibility to reassure passengers that security is taken seriously and giving the impression that there is a high security risk. Any measures introduced must be considered for their acceptability to passengers and non-passengers. The higher the acceptance of a security measure, the higher the corresponding improvement of the experience will be.

In general, an approach likely to win staff and customers' confidence is to provide visible patrols, install technical solutions that do not affect passenger flows and provide staff and customers with information on the benefits and meaningfulness of particular measures.

Non-intrusive processes, security culture, security by design, and a combination of uniformed and plain-clothes behavior detection officers along with constant, passive surveillance have been identified as effective measures that maintain passenger experience and operational efficiency.

5 EMERGENCY PREPAREDNESS AND RESPONSE

Preparing for and responding to any emergency are cornerstones of effective airport landside operations and should be a significant consideration in any airport operator's daily activities.[4] Emergency preparedness and response can be defined as anticipating, evaluating and taking corrective action in order to coordinate and contain a crisis situation of indeterminate size and impact. Effective emergency-response operations require thorough pre-event planning; broad stakeholder and community engagement and participation; and a clear understanding of roles and responsibilities before, during, and after an event has occurred.

Preparedness can include planning, training, and identifying resources that will be needed and available to save lives and support an efficient response to an emergency event. Successful preparedness, response, and resumption of operations can be achieved through three specific activities:

1. Performing detailed pre-event planning to mitigate the impact of an event and expedite the response when an event occurs;
2. Providing an organized response in order to control and resolve the emergency in a timely manner, with minimal damage and impact to operations; and
3. Developing extensive recovery plans that facilitate a thorough and quick reconstitution of operations. (Recovery is discussed in more detail in Chapter 6.)

Robust planning is key and should include development of detailed and precise procedures that are well understood within the airport organization and across the airport community. Robust planning and discussion before an event occurs will limit confusion, streamline task delegation, and expedite the assignment of critical emergency responsibilities for key personnel during a crisis or emergency event.

In this chapter, we will discuss how to prepare for and respond to an emergency event and explore ways by which an airport can position itself to deal best with such an event. These strategies will be discussed with an eye toward expedited and effective response, minimizing damage, increasing personnel safety and re-establishing normal operations in a safe and timely manner.

5.1 Airport emergency-response plans

Effective emergency-response plans are critical in saving lives, minimizing damage, and resuming operations in a timely manner. When developing emergency-response plans, it is important to take an all-risks approach, defining scenarios that allow for considerations based on the nature of the event. A terror attack requires immediate action and a coordinated response, and these requirements may have implications for the planning process based on there being a need for external-authority participation in the event. Ensuring effective responses to differing scenarios requires that plans be effective, whether or not there is any warning of an event; that they take into account continuity of operations, such as providing alternate facilities; and that they define timelines and expectations for resumption of operations.

Ensuring participation by all stakeholders and community partners in preparedness-planning activities will help facilitate quick and concise action when an event has occurred. These planning activities include:

- Helping various stakeholders understand their roles and responsibilities when an emergency occurs;

[4] Regulation (EC) No 300/2008 of the European Parliament and of the Council defines "landside" as those parts of an airport, adjacent terrain and buildings or portions thereof that are not airside; "airside" is defined as "the movement area of an airport, adjacent terrain and buildings or portions thereof, access to which is restricted."


VA1741 ALICE SPRINGS 1350 CLOSED 15
QQ854 MOOMBA 1400 GO TO GATE 26
QF2271 PORT LINCOLN 1400 CLOSED 50
QF1877 KALGOORLIE 1405 CLOSED 21
VA719 PERTH 1410 FINAL CALL 12
QF684 MELBOURNE 1410 FINAL CALL 20
QQ4547 PROMINENT HILL 1415 GO TO GATE 50
VA1397 BRISBANE 1430 14
QF756 SYDNEY 1445 24
QF690 MELBOURNE 1455 21
QQ3214 OLYMPIC DAM 1500 50
VA427 SYDNEY 1500 15
TT464 MELBOURNE 1500 23
ZL4382 PORT LINCOLN 1505 10
VA228 MELBOURNE 1505 13
JQ974 PERTH 1510 GO TO GATE 22
ZL4631 MOUNT GAMBIER 1540 10
QF664 BRISBANE 1550 20
ZL4536 WHYALLA 1600 10
#GettingTh
#OneStepO

- Identifying needs and requirements that might otherwise go unnoticed until an emergency occurs;
- Ensuring that mission-essential functions continue and that impacts on operations are mitigated to the extent possible;
- Increasing protection of facilities and personnel; and
- Facilitating orderly and timely reconstitution of operations.

When developing an emergency-response plan, it is important that its key assumptions are validated. This step allows stakeholders and key emergency personnel to gain a shared vision of the potential impacts of an event across operations and stakeholder communities. An open and detailed discussion of the following questions will assist in defining, validating, or disavowing commonly held assumptions and will support thorough and effective planning activities:

- What are the various types of disruptions that might occur? Are there opportunities for early warnings in any of the scenarios?
- What facilities and materials will be accessible during the event, if any?
- Do back-up systems for information and communications exist and do stakeholders and community members know how to access them? Are these systems tested routinely?
- Will employees and stakeholders know where to go when an event occurs? Have they been educated on various evacuation, shelter-in-place, and other emergency plans?
- How will key personnel get to alternate/remote facilities?
- Do common communication platforms exist for notification of emergency or reconstitution orders?
- Do employees and stakeholders know how to notify law-enforcement personnel of an emergency at the facility? Is it easy to describe the location of where an event is occurring?
- How will the public be directed on how to respond during an emergency? Are evacuation areas clearly marked and described?

Several key elements should be incorporated into an emergency-response plan. These elements are:

- *Base plan*—The base plan provides an overview of the airport's emergency response organizational structure, discusses the authorities on which the plan is built, provides a general concept of operations and outlines roles and responsibilities of key emergency-response personnel;
- *Operational annex*—The operational annex section discusses communication protocols and outlines specific operational-response actions by different organizations and groups, including law enforcement, emergency medical and public works organizations;
- *Scenario-specific plans*—These plans provide operational-response activities associated with specific events or incidents and are considered stand-alone documents within the larger emergency-response plan; and
- *Procedures and checklists*—This section contains detailed instructions for individuals or organizations to take during an event and supporting checklist documents. These instructions and checklists are typically hazard-specific and should be as detailed and as thorough as possible.

Plans should be developed in coordination with all key stakeholder and community partners within an airport facility. Stakeholder communities that should be considered during development of the plans are:

- Hospital and medical services;
- Rescue and firefighting services;
- Government authorities;
- Multi-modal transportation authorities;
- Military branches;
- Public utilities;
- Air traffic services;
- Airport authority;
- Communication services;
- Rescue coordination centres;
- Public information office;
- Airport volunteer personnel;
- Police and security services;
- Aircraft operators;
- Airport tenants;
- International relief agencies;
- Mental health and crisis-support services; and
- Airport vendors and service providers.

Emergency response plan components			
Base plan	**Operational annex**	**Scenario specific plan**	**Procedures and checklists**
Authorities, delegation of roles and responsibilities, general concept of operations	Communications, emergency operations, public health, resource management	Scenario specific authorities, responsibilities, and actions	Detailed instructions, procedures, and checklists to support emergency operations

Emergency-response plans should be readily available to all key personnel in the airport organization and should be updated on a routine basis. If possible, they should be maintained in both paper and electronic formats to facilitate ease of access for individuals, including during periods when routine access to computer systems may be affected. Plans should be drilled on a routine basis and lessons learned should be continuously incorporated into the existing plans. Lastly, it is imperative that plans incorporate emergency-contact information for all key personnel and stakeholders and that this information is updated as changes occur.

5.2 Scenario-specific plans

While all aspects of the emergency-response plan are critical, careful attention should be given to scenario-specific plans to ensure that they are robust and provide clear delineation of roles and responsibilities and procedures during a specific type of event. Scenario-specific plans include:

- A general description of the event;
- The purpose of the specific plan;
- Assumptions associated with the specific scenario;
- Roles and responsibilities of personnel and organizations under the specific planning scenario, including definition of the chain-of-command structure;
- A discussion of what logistics will be provided and by whom during the event;
- Standard operating procedures and checklists specific to the event; and
- Identification of the responsible point of contact for maintenance and update of the plan.

As discussed, airport authorities should take an all-hazards approach to emergency operations planning. Emergency situations to consider and plan for include, but are not limited to:

- Criminal activities affecting employees or passengers;
- An insider threat;
- An active shooter;
- Explosive devices outside the terminal building;
- Explosive devices within the terminal building;
- Bomb threats;
- A hostage crisis;
- A hazardous materials (HAZMAT) release;
- A chemical, biological or radiological attack;
- System and/or facilities failures;
- Fire, flooding, or smoke damage;
- Weather emergencies;
- An on-property aircraft accident;
- Breaches to the perimeter fence line; and
- Attack by man-portable air defence systems (MANPADs, also known as shoulder-launched missiles).

EMERGENCY PREPAREDNESS AND RESPONSE

The following is an example of an active shooter scenario-specific plan. The contents of this plan will largely be dictated by the authorities of responding law-enforcement agencies, but the example gives a general overview of how the various sections of the plan translate into scenario-specific information.

Hazard-specific plan – Active shooter

General information:
Active-shooter incidents can occur without warning in any area of the facilities or properties located on the airport. An active shooter is defined as an individual actively engaged in killing or attempting to kill as many people as possible in a confined and populated area. In most cases, active shooters use firearms and there is no pattern or method to their selection of victims. Nor do they care about surviving the event.

Purpose:
The information and guidance contained in this scenario-specific plan supplements the Basic Airport Emergency Plan and Operational Annex. This specific plan defines authorities, responsibilities, and actions to be taken in the event of an active-shooter event in the airport.

Assumptions:
- All active-shooter reports will be taken seriously until they are validated or resolved by law-enforcement authorities.
- One or more law-enforcement agencies will be the primary responders to the event and airport operations will assume a support role.
- Portions of the airport will be treated as a crime scene and ingress and egress will be hindered for an undetermined amount of time.
- Aircraft operations will be disrupted for an undetermined period of time. The airport should be prepared to operate with limited air service for several days, based on the time necessary to process the crime scene.

Organizational responsibilities:
Law-enforcement agency
- The law-enforcement agency is the primary responder to the active-shooter incident. It is responsible for overall command and control during an active-shooter event.
- The law-enforcement authority will execute a plan to deter, respond to, and recover from the event.
- The law-enforcement agency is responsible for traffic control and maintains all authority for ingress and egress to the scene, including pre-planned alternate routes in the event primary routes are blocked.

Emergency medical services
- The emergency medical services are responsible for all medical service aid rendered at the scene and for handling of all casualties and injuries which occur as a result of the event.
- Emergency-services vehicles should have pre-planned routes so they can reach injured parties in the event that normal traffic roads are blocked due to stalled traffic.

Airport authority
- The airport authority is responsible for implementing the airport emergency plan.
- The airport authority is responsible for activating the emergency operations centre.
- The airport authority is responsible for directing the cessation or diversion of all operations on the airport property.
- The airport authority is responsible for assisting in operations, including accountability and safety actions.
- The airport authority is responsible for activating public address or alert-warning systems to notify employees to seek safe locations and to stay away from impacted areas.
- The airport authority is responsible for implementing personnel-support systems and providing locations for impacted personnel and family members.
- The airport authority is responsible for issuing identification media, in advance, that will restrict access to impacted areas for those other than emergency personnel and first responders.

Air traffic authority
- The air traffic authority will coordinate movement of all aircraft on the airport grounds, including ordering the hold of all ground and air operations.
- The air traffic authority will coordinate the movement of emergency air units for access to the facility/scene.

Aircraft operators
- Aircraft operators will support all emergency operations and adjust their operations, as directed by the air traffic authority and the airport authority.

Airport public information officer
- The airport public information officer will provide public messaging via media outlets, in coordination with law-enforcement authorities.
- The airport public information officer will coordinate with other public-information authorities to ensure a unity of message.
- The airport public information officer will monitor media accounts to ensure awareness of ongoing events by airport personnel and the public. The public information officer should use all media engagement tools available, including social media.

Airport tenants and vendors
- Airport tenants and vendors will adhere to all evacuation or shelter-in-place orders and protocols.

Logistics:
Primary logistical support for the response to an active-shooter event will be provided by the law-enforcement agency. The airport authority will provide broad logistical and administrative support at the request of the law-enforcement entity, as appropriate.

Standard operating procedures and checklists:

Law-enforcement reporting information

Information to provide to law-enforcement officers or dispatchers includes:
- The shooter's location;
- Callers' locations;
- The number of shooters;
- Whether law-enforcement officers are on site and description of all LEOs on site, including their uniform markings;
- Physical description of the shooter(s);
- The type(s) and number of weapons used by the shooter(s);
- Numbers of shots fired;
- Use or threat of explosive and description of type of explosive—key switch, dead-man switch, suicide vest, etc.;
- Whether shooting is still occurring;
- The number of potential victims at the scene;
- A map of the facility;
- Access to media or master keys; and
- Video footage of the airport.

Employee response guidance, such as run, hide, fight

Include all guidance provided to employees regarding their response to the active-shooter scenario. In this situation, videos should be used if at all possible.

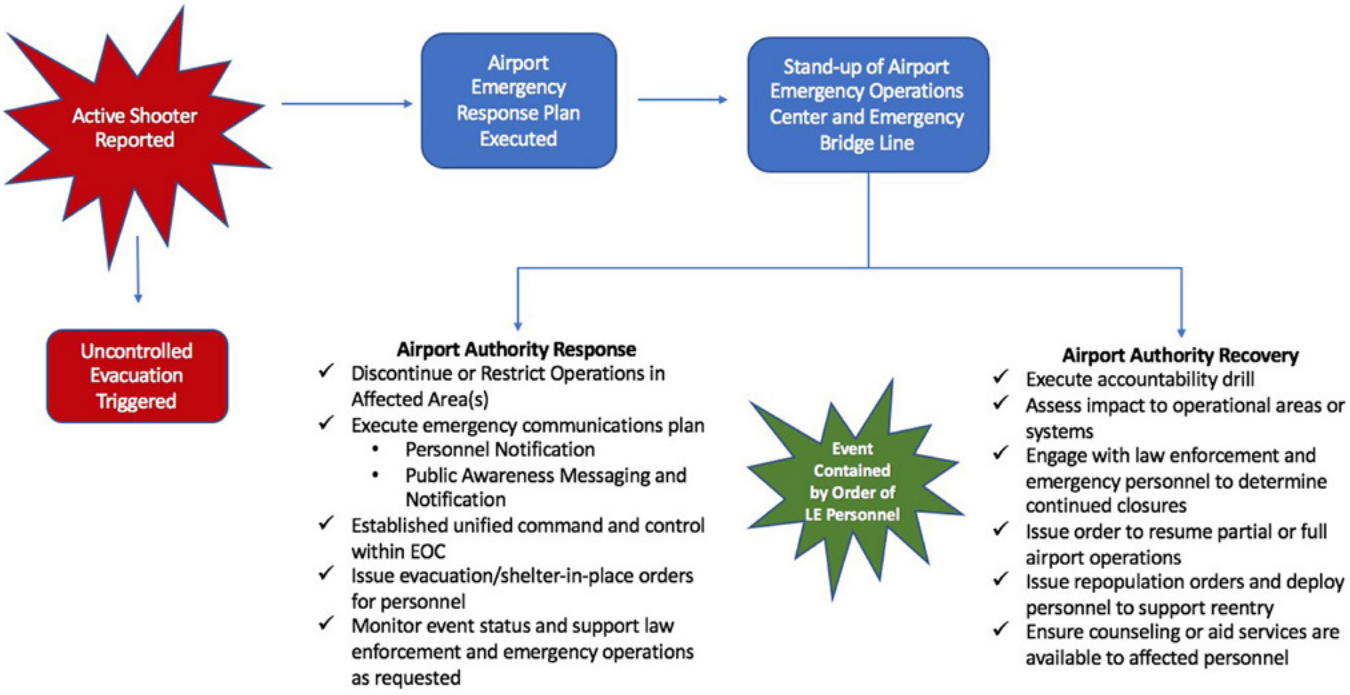
Evacuation, shelter-in-place, and lock-down locations

Include maps and graphics of all evacuation, shelter-in-place, and lock-down locations.

For terrorism and criminal events, it is important for airport authorities to consider threat reporting as being credible until it is validated, substantiated and/or resolved by a law-enforcement authority. There can be a delay between the reporting of a threat and the establishment of its credibility, so it is critical for airport authorities to remain engaged with law-enforcement authorities and other stakeholders and to monitor actively all reporting on the matter, in order to make informed decisions regarding the safety of their employees and continuity of their operations. Initial reporting in these scenarios is not always complete or clear, so maintaining flexibility of response and increased awareness is critical.

5.3 Defining roles and responsibilities

A crucial step in the preparedness process is to define the roles and responsibilities of key personnel. This step should be accomplished at multiple layers of an airport organization and the airport community. It is important to define roles and responsibilities internal to an organization as well as across communities and stakeholder groups. This step is best achieved by establishing Emergency Response Planning Teams that incorporate broad portions of the potentially impacted communities. These planning teams will increase cooperation and communication among stakeholders



and ensure that the plan incorporates numerous perspectives and equities.

Key personnel should be listed in emergency-response plans and their individual key functions, authorities, and responsibilities should be clearly delineated and discussed. The goal is to ensure that, when an emergency occurs, all key staff members understand and execute their roles and are knowledgable of the roles of others within the organization. These persons should ensure that all within their organization are trained and have awareness of emergency responsibilities for themselves and their organization.

Key emergency personnel

Defining critical roles of key personnel during an emergency will expedite orderly evacuations; minimize operational disruption to the greatest extent possible; ensure the safety of employees, airport personnel and customers; and allow for the most timely reconstitution of operations at the airport or facility. Multiple stakeholders should be considered when defining roles and responsibilities. These will include:

- Airport and air carrier management;
- Air traffic authorities;
- Law-enforcement and emergency personnel;
- National and local government organizations;
- Intelligence organizations;
- Public-information staff; and
- Aid organizations.

Emergency-response plans should clearly delineate the roles and responsibilities of each organization which is included and annotate whether each serves in a primary or a support role for those functions for which it is designated. The plan should also include the authorities under which these functions are exercised, so that there is no confusion amongst multiple stakeholders regarding the ability or right of an organization to act in a particular manner during an emergency event.

A master emergency-contact roster should be developed, maintained and exercised on a routine basis. The contact roster should list primary and back-up points of contact for each responsible organization and/or division. Contact rosters should include names,

Airport canine unit checking baggage – Courtesy of Aéroports de Montréal

positions, routine and emergency phone numbers, and alternate points of contact for each position.

Practice drills using the emergency rosters should be conducted on a routine basis, including implementing quarterly call-tree exercises to ensure that key personnel are reachable and that they are familiar with the notification processes.

Orders of succession

Orders of succession identify individuals who have primary responsibilities for executing emergency plans and who have decision-making authority during an emergency event. It is important for operators to consider whether everyone listed in the order of succession is located in the same place and whether persons outside of the airport's immediate geographical location (i.e. those located at remote facilities) are needed to serve in decision-making roles if local decision makers are incapacitated or unavailable.

An example of an order of succession for an airport's executive leadership is as follows:

1. Airport director;
2. Deputy airport director;
3. Director of airport operations;
4. Airport operations manager;
5. Airport operations supervisor; and
6. Remote airport operations personnel.

It is important to share the order of succession throughout impacted stakeholder communities within the airport and that they share their plans as well. The ability to understand who has authority in emergency situations, how to contact them, and the locations of those individuals during an event will significantly decrease response times and increase communication flow. Additional considerations that should be made when establishing orders of succession include:

- Do personnel in the succession plan understand their roles and responsibilities during an event?
- Do personnel in the order of succession have ready access to materials and communications equipment that they will need to execute their responsibilities?
- Do personnel have the right identification media and credentials to gain access to all areas during an emergency?
- Are emergency personnel at the facility aware of the order of succession and protocols that establish shared expectations about decision-making during an event?
- Has each individual in the succession participated in drills and exercises to ensure that he/she can execute his/her responsibilities during an emergency?

5.4 Considerations for emergency communication

Orderly communication during an emergency event is critical to ensuring that emergency responders have the information they need to support decision-making and that critical information is received by those who need it in real-time, with minimal disruption. Establishing communication protocols and systems and training key personnel as part of the airport's preparedness activities will serve as a foundation for effective response to any emergency event. Key communication tools to consider include mobile and landline phones and internet capabilities, together with dedicated emergency phone numbers and storage folders for plans and other materials. Airport operators should also consider establishing redundant communications and file-sharing systems should primary methods of communication fail or be otherwise disrupted.

Separate communication systems should be established for key personnel than those used for routine communication during an event. This will facilitate open communication and controlled exchange of information between those individuals who are acting in decision-making roles. Proper communication etiquette and protocols are necessary and must be practiced by those participating in emergency calls. Airport operators should also consider establishing a central leadership role in facilitating the conference calls so that messaging is managed and controlled and communication can occur in an orderly fashion. Additionally, a note-taker or recorder should be assigned to maintain a record of events during the call or meeting.

The importance of ensuring that communications systems are interoperable across various stakeholders cannot be stressed enough. Multiple real-world incidents have underscored the important role that pre-defined common communications systems, channels, and protocols can play in providing effective responses to events and in expediting the recovery following an event.

Where and when possible, communication should be made in person, in a room or facility that is dedicated to emergency-management activities, such as an emergency operations centre. Specific provisions should be made for this type of facility, including:

- Availability of communications equipment;
- Availability of primary and back-up power resources;
- Availability of emergency plans and materials;
- Availability of television and radio systems;
- Availability of basic facilities and resources (restrooms, meeting rooms, etc.); and
- Availability of supplies (office supplies, clocks, diagrams).

Access to an emergency-operations facility should be restricted to key personnel and dedicated positions should exist for each organization. Key personnel should be familiar with the facility, its access protocols and all its other features.

It is important to establish expectations regarding roles and responsibilities associated with the establishment of emergency conference calls or other communication events. Best practices in this area include the establishment of call trees, either triggered electronically through commercial systems or manually by

Operations control centre – Courtesy of Montevideo Airport

individuals who are assigned responsibilities to initiate emergency notifications. Call-tree maps should be created and should identify by name all persons who are responsible for cascading emergency notifications. Consideration should be given to delegating call-tree notifications to non-key emergency personnel so that key personnel are not distracted from their emergency decision-making responsibilities. It is important for key personnel or organizations to understand what is expected of them when they receive a notification and if any acknowledgement of the notification is required. The emergency call tree should be available broadly and should be included in emergency plans and intranet or internet file-sharing locations for emergency response. Call trees should be exercised on a routine basis and new personnel should be trained on expectations regarding emergency-notification protocols.

5.5 Key decision-making responsibilities

Authorities who have responsibility for decision-making during an emergency event will be from multiple organizations and their individual participation may be dependent on the scenario that is occurring. For example, the emergency personnel responding to weather events will be significantly different from those responding to acts of terrorism. Authorities that maintain decision-making roles in these situations can include airport authorities, foreign ministries and police and government authorities, all of whom have different authorities and responsibilities within a single jurisdiction or area.

As discussed in the preceding section, an emergency operations centre should be established to allow for central command and control of an emergency event. Leaders must be able easily to consider, approve, monitor and coordinate actively the actions taken during the event. Airport operators should consider establishing an Incident Commander position in the emergency operations centre to facilitate the flow and sharing of information. There are many options for organizing an emergency operations centre and all such options should be carefully considered. Best practices in this area include organizing around functional areas such as operations, resource management, logistics, and planning, so that actions are coordinated in a meaningful way across the airport organization and authorities that share common functional requirements or areas of expertise.

There are many important roles to consider in providing effective emergency management within the airport organization. Airport operators should establish Emergency Response Teams, which may consist of the following positions:

- *Designated official*—The designated official has primary decision-making responsibility to direct the implementation of emergency plans. This individual has final decision-making authority for all areas within his/her organization's domain.
- *Emergency-response coordinator*—The emergency-response coordinator is responsible for ensuring personnel at all levels have copies of emergency response plans; that the plans are exercised at regular intervals; and that emergency-response team members are trained in all the procedures for emergency scenarios.
- *Occupant emergency coordinator*—The occupant emergency coordinator is responsible for overseeing emergency-response personnel who are engaged during an emergency to ensure the safety of personnel in different locations and to minimize damage during an emergency event. The occupant emergency coordinator can have supporting teams that can include terminal, elevator and ramp monitors for emergency scenarios.
- *Public information officer*—The public information officer is responsible for developing and providing clear, coordinated, and accurate public-facing messaging regarding emergency events and responses.
- *Incident commander*—The incident commander is responsible for providing operational oversight in the emergency operations centre and on key-personnel conference calls to ensure that communication and information is managed in a way that optimizes response operations.

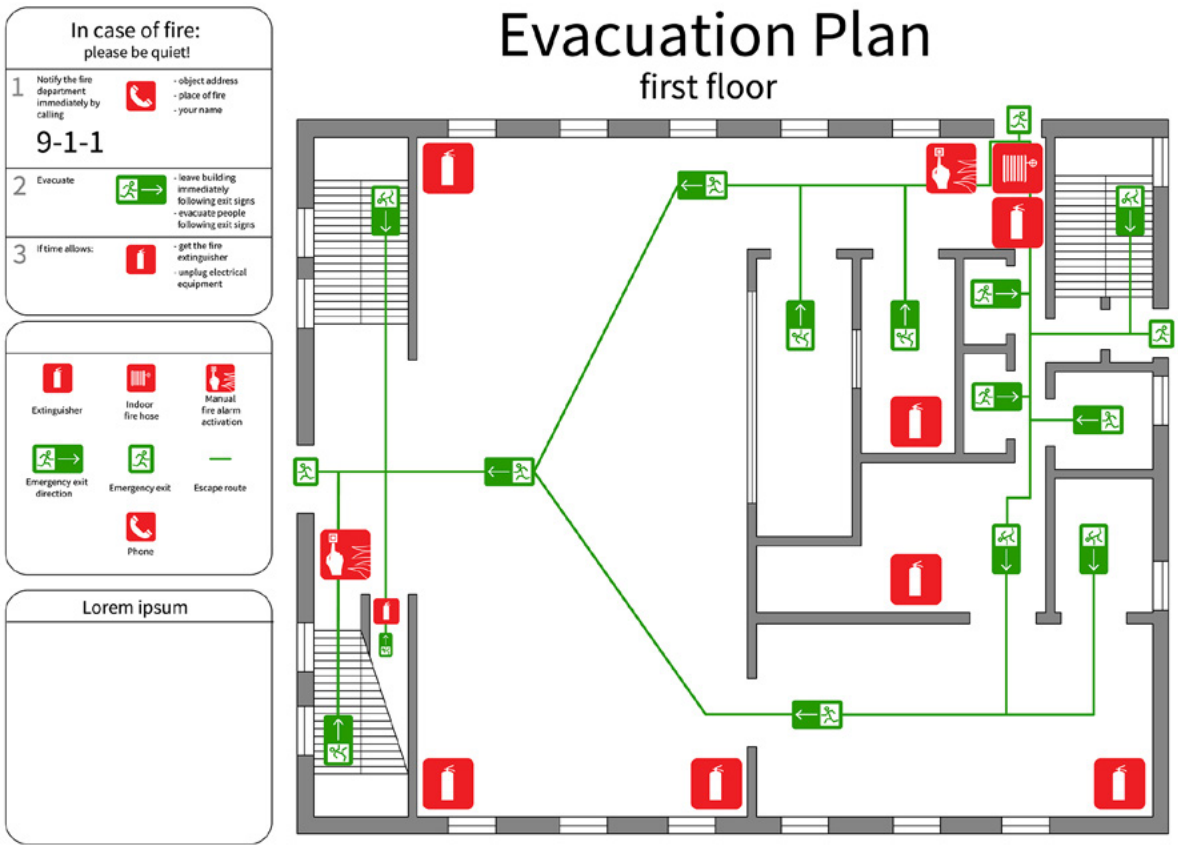
Airport operators should consider what key emergency-personnel positions may best support their operations during an emergency or crisis event. It is imperative that individuals named to these key positions also be provided with the requisite training and skills to succeed in their designated positions.

5.6 Evacuation plans

An evacuation plan is essential in preparing for and responding to an emergency event. Evacuation plans should be well understood by airport and emergency personnel; clearly marked throughout public spaces within the airport; and readily available to first responders such as police officers, fire fighters and emergency medical personnel. Airports should consider publishing their evacuation plans so that they are available to personnel, tenants and passengers.

When developing an evacuation plan, a comprehensive understanding of the physical layout of the airport or facility is vital. Key emergency personnel should have intimate knowledge of the physical footprint of the airport so that they are able to provide an effective response to an incident occurring at any specific location within the airport perimeter. This knowledge will ensure that decisions are made with consideration to physical characteristics such as ingress and egress routes, proximity to shelter locations and medical equipment, and potential alternate-access areas that need to be secured or opened based on the nature of the event. Awareness of the physical layout of the airport will also support the crowd-control measures crucial in managing an incident.

Evacuations in airport facilities can occur either in a controlled manner based on notification of an incident or without purposeful initiation because of an actual or perceived threat to individual safety. Additionally, evacuations can be partial or complete, depending on the nature of the event. Emergency planners should consider both scenarios when developing an evacuation plan for the airport. Common meeting areas



should be established in locations that have been pre-approved and that offer the safest places for assembly during an emergency. Airport operators may also consider areas that do not have many windows; that are in remote, but accessible, locations; that can hold large numbers of people; and that are comparatively resistant to forced entry.

Pre-determined rendezvous points such as ingress and egress routes for fire-truck and ambulance crews should be established to allow for rapid deployment of emergency vehicles. This will be particularly important in the event of an explosion or other high-casualty event that requires a rapid response. For these reasons, public stand-off areas should be established at a set-back, in order to facilitate ease of access to the event by first responders. Consideration should be given to traffic patterns and the closure of ingress routes to prevent additional crowding in the area of the emergency.

Airport operators should be mindful of evacuations that may occur because of false alarms and should work to avoid or mitigate these scenarios to the extent possible. Establishing clear visual and audible communications that provide information to personnel and to the public and allow individuals to remain aware of false alarms and calm are vital in minimizing the impacts of evacuations caused by false alarms. Each false-alarm evacuation should be the subject of immediate review, to determine actions that may avoid future false alarms or further mitigate evacuations as a result of false alarms.

There are many recent examples of uncontrolled, self-initiated, mass evacuations in the airport environment, either for perceived or actual threats to personal safety. During these events, it may be challenging to implement normal evacuation procedures and use of pre-defined locations. These challenges can be mitigated by having trained airport employees available to provide direction and assist with crowd control. Airports can and should consider expanding or creating additional evacuation points that are further away from the terimal. Since the airport will probably be closed to air traffic at the time of the event, the airport should coordinate a response by airport operations, maintenance, and law-enforcement personnel who are familiar with operating on the airport operations area (AOA). These individuals should be in vehicles with public address systems so they can communicate better with staff. Personnel assisting in this capacity should direct others to alternate evacuation locations away from the impact areas.

Airport authorities need to give significant consideration to mass evacuations and methods to mitigate the impacts during these events. Some actions that can minimize impacts are:

- Ensuring effective, coordinated information-sharing between law-enforcement and security personnel regarding the credibility of the event;
- Ensuring that during a mass escape event, emergency access doors are immediately released to allow for emergency staff and law enforcement to easily access areas involved with emergency event
- Providing robust passenger communication capabilities and protocols, including public announcement and broadcast systems, which can also be used in vehicles to support evacuations on the AOA;
- Conducting advanced training for airport personnel on engagement with passengers during evacuations;
- Making broad and immediate use of social media to report the nature of the threat, particularly if it has been verified to be not credible;
- Using alert-warning systems or text-message systems to notify personnel of an event and all associated instructions and information; and
- Performing immediate review and lock-down of video to offer information to law-enforcement personnel regarding the credibility of the threat communities in identifying any additional information regarding the event.

It is important to note that, as mentioned in section 5.2, criminal and terrorism threats should always be assumed to be credible until otherwise validated by law-enforcement personnel. While disruptions during self-initiated mass evacuations can be significant, ensuring people's safety and security is of primary importance. That being said, once it is determined that safety and security of the evacuees has been established and no threat exists, people should be allowed to leave the area on their own accord in a safe manner.

A resource to consider on this topic is the Fort Lauderdale Hollywood International Airport (FLL) Active Shooter Incident and Post-Event Response report dated August 15, 2017, which can be found here: http://www.broward.org/Airport/Advisories/Documents/Afteractionreportfll.pdf. This report discusses lessons learned from the January 6, 2017, shooting at FLL which resulted in a real-world mass evacuation of people. It offers excellent insight into considerations that should be assessed by airport authorities and stakeholders when developing evacuation and emergency-response plans.

5.7 Back-up systems and processes

Identifying critical systems in advance of an emergency and establishing redundant capabilities for those critical functions will be vital for the timely and effective resumption of service and operations following an emergency event. Primary operational systems may be impacted for long periods of time depending on the nature of the event and this may hinder operations significantly. Airport operators should identify critical systems and capabilities during the emergency-planning process; routinely test activation of back-up or redundant systems to ensure their operability on a real-time basis; and actively use these systems at peak times of normal operations to ensure that, during an emergency, they are capable of supporting the full load of operations and activities.

When planning for redundant capabilities, consideration should be given to:

- Loss of power;
- Structural damage or loss;
- Loss of network connectivity; and
- Loss of voice-communication capability.

Airport operators that incorporate all-hazards scenarios into their planning processes will be well-positioned during recovery phases to begin operations in a timelier and more complete manner.

5.8 Summary

Effective preparedness and response-planning activities can minimize impacts to operations, save lives and ensure thorough and timely reconstitution of operations at an airport facility. By performing thorough pre-event planning and broad stakeholder and community engagement, and delineating roles and responsibilities before, during, and after an event has occurred, airport operators can optimize their responses to emergency events or crisis situations.

These key activities will ensure an effective response to any emergency:

- Have an emergency operations plan and ensure it is broadly available, thoroughly understood and exercised on a routine basis;
- Establish an emergency-response planning team which includes broad participation from stakeholders and members of the airport community;
- Outline roles and responsibilities clearly and conduct training for personnel to ensure that all members can be successful in their roles during an actual event;
- Define communication channels and notification protocols in advance and exercise them regularly to ensure that emergency and non-emergency personnel alike understand their roles and how to respond in the event of an emergency;
- Establish decision-making roles and responsibilities and ensure that they are included in the emergency-response plan; and
- Design, develop, and implement evacuation plans that consider multiple scenarios, leverage the physical footprint of the airport and optimize life-saving opportunities.

6 RECOVERY

After an emergency has occurred and effective response protocols have been implemented, airport operators and other decision-making officials will naturally turn their attention toward the resumption and reconstitution of operations. Distinct from the emergency-response phase, this phase, commonly referred to as recovery, focuses on issues that arise after immediate needs are addressed. The recovery phase centres on restoring normal operations, repopulating public and secure areas while being mindful of ongoing investigatory and facilities impacts, and ensuring that staff members and other impacted individuals have confidence that they are safe. Additionally, recovery also offers a time to reflect on the event that has occurred and to gather leaders and those affected to identify ways to improve for future events and to further refine plans and activities for emergency situations. This last step is often overlooked, but is one of the most meaningful activities an organization can undertake following an emergency event.

6.1 Declaring the airport safe

Declarations regarding the ending of an emergency event are some of the hardest decisions that key personnel will have to make during an emergency. Decision-makers must consider many factors when issuing "all clear" declarations and when resuming full or partial operations at the airport or facility. Like the preparedness and response phases, recovery requires broad participation by stakeholders and community members to ensure that a full perspective of ongoing activity and impacts is being considered. While the authority to resume normal operations may rest with one individual, multiple individuals and organizations maintain the responsibility for recovery and all of them should be factored into any decision regarding reconstitution of operations. Some considerations are:

- What facilities are impacted and how does that directly affect the resumption of service?
- Is all technical and communications equipment available and, if not, what back-up systems need to be established to resume normal operations?
- Are mental health professionals ready and available to affected personnel?
- Have authorities completed their investigation of the event? If not, what are the physical perimeters of the investigative area that will remain closed?
- Do I have a full accounting of all resources and equipment following the incident?
- Do I need to call in additional personnel to augment those that might be impacted by the emergency event?

The first step in declaring an airport or facility safe is to conduct a thorough inspection of the affected locations, to ensure that the area is free of safety hazards and is fully capable of supporting operations. Notifications will need to be made to all affected stakeholders that the airport is about to be declared safe, to ensure there are no concerns on the parts of impacted organizations or personnel. Also, consideration needs to be given to customer and passenger notifications and announcements to ensure controlled repopulation of facilities and awareness of potential ongoing impacts from the event. Additionally, repopulation of public areas should be supported by airport staff to ensure orderly re-entry into the building and other facilities so that service and support organizations are not overwhelmed.

6.2 Roles, responsibilities, and criteria for recovery operations

Once the emergency response has concluded, local officials will normally begin the recovery phase of the event. Several key roles should be considered in any recovery plan. Ensuring formal designation of these roles and providing training and information to those individuals who perform them can expedite recovery operations. Some key roles to consider are:

- *Recovery coordinator*—A recovery coordinator should be identified in advance for recovery efforts. This individual will implement the recovery plan and coordinate across the various stakeholders and community organizations to ensure unity of effort and effective sharing of information and, where appropriate, resources.

- *Emergency recovery unit*—Similar to an Emergency Response team, the emergency recovery unit is responsible for providing operational and logistical support during the recovery phase. This unit is led by the recovery coordinator and will directly implement various aspects of the emergency recovery plan.

- *Crisis communication coordinator*—A crisis communication coordinator will manage public and internal messaging, coordinate amongst various stakeholders regarding media and other communication inquiries, and develop robust communication plans to inform multiple stakeholders—among them the airport's staff members and the public.

- *Emergency services coordinator*—An emergency services coordinator can be assigned to provide a single point of contact and a method of coordination across emergency service providers—among them fire, police, and rescue personnel.

- *Engineering and facilities coordinator*—An engineering and facilities coordinator can be assigned to serve as a single point of contact to manage public-works and facilities-oversight requirements. The duties of the coordinator include coordination of restoration of facilities, services and resources.

While often not under the immediate direction of airport personnel, additional groups and organizations that need to be considered and given a voice in recovery operations are:

- Hospital and medical services;
- Air traffic services;
- Police and security services;
- Rescue and firefighting services;
- Airport vendors and service providers;
- Aircraft operators;
- Government authorities and communication services;
- Airport tenants;
- Multi-modal transportation authorities;
- Rescue coordination centres;
- International relief agencies;
- Military public information offices;
- Mental health and crisis-support services;
- Public utilities; and
- Airport volunteer personnel.

6.3 Considerations for crime scenes and investigations

In any criminal or terrorism-related emergency event, investigation activities are likely to extend well beyond the period of time when normal services are resumed. It is important that airport and facility operators give consideration to this fact when developing and executing recovery plans. Crime-scene investigations can require buildings, facilities, and roadways or parking garages to remain closed for extended periods, necessitating alternate arrangements for those specific locations. The areas affected by the emergency should be cordoned off to facilitate and support the needs of investigators. These areas will probably remain under the authority and jurisdiction of police and government agencies for the duration of the investigation.

Airport operators can both support the need for thorough investigation and pursue resumption of operations if they give consideration to the use of alternate facilities (see Section 6.4 below for more discussion on using alternate facilities to support operations) and phased reopening of operations. For example, an emergency event that occurs in one terminal may result in only minimal impacts to adjacent terminals at the airport. Airport operators can work with aircraft operators' staff to move operations to nearby terminals to support continued operation. It is imperative that airport personnel remain in direct contact with the lead investigating agency to ensure that crime-scene investigations are not impacted during routine-service operations. The integrity of the investigation should be of utmost importance in all decision-making regarding recovery and reconstitution of operations.

6.4 Use of temporary facilities

Airport staff should anticipate which areas should begin resuming normal operations so that resumption occurs in a logical and controlled order. Access to buildings and facilities may be hindered during recovery operations, so consideration should be given as to how operations will be prioritized and whether temporary or alternate facilities can be used to achieve partial operations. Considerations for airport staff include the fact that available physical space, food and vendor services will all be reduced, as will be facility resources; and that these reduced resources will be required to support larger volumes of people and passengers in smaller areas of the airport.

In some emergencies, locations and buildings that support critical operational functions can be damaged or destroyed. In their planning processes, airport operators should consider the location of critical services and identify redundant locations for those support services. For example, if coordination centres are closed, alternate facilities that are equipped to support those functions should already be identified and should be stood up as redundant services in temporary locations when an emergency is unfolding. Planning for and establishing temporary or alternate facilities in advance of an emergency can make a significant difference in recovery timelines and ultimately in the resilience of the airport in an emergency or crisis.

6.5 Personnel confidence and safety

Airport operators should maintain a roster of all the personnel who are on duty at any given time. Should an emergency event occur, this allows for immediate accountability for all on-duty and on-location staff who might be affected by the event. Employee accountability efforts should continue until every employee is accounted for after the event.

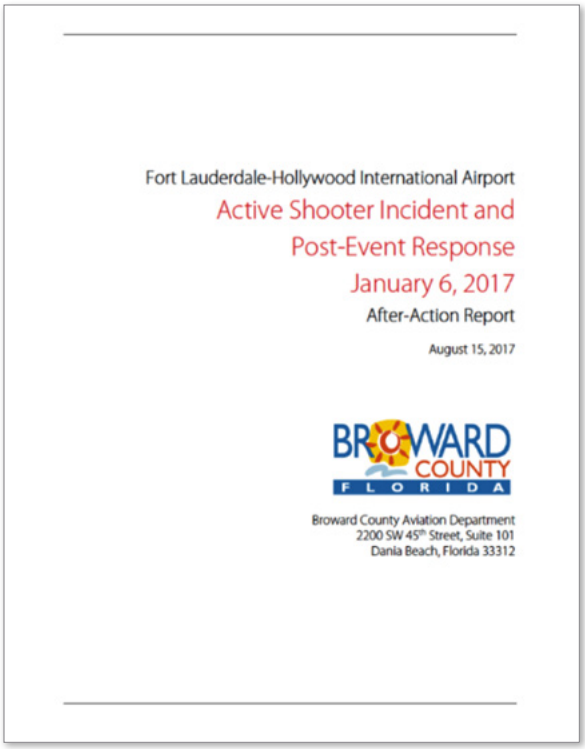
It is normal for staff members to feel concerned and scared following an emergency event and it is critical that leaders within the organization assure the safety of the staff and bolster their confidence about returning to their place of work. These employees will be critical in providing an effective recovery, so taking care of their needs and health will be a critical step in the recovery plan.

Commonly, staff members who are present during the event will experience some form of shock, confusion, or grief associated with the emergency. They should be offered both medical and psychological support immediately after an event and continuing through the following days. Mental health services should be made available to staff members to assist them in coping with the traumatic experience. Additionally, consideration should be given to bringing in staff from another location—a sister-city airport, for example—to support operations while the affected airport's staff members work through the impact of what has occurred at their place of work and the potential impacts to their co-workers. Also, faith-specific religious representatives should be available in the event that any employee expresses his or her need for spiritual guidance to help him or her cope with the event.

6.6 After-action review

After-action reviews of emergency events and actions are critical to the planning and preparedness process. Collecting from and discussing lessons learned by all stakeholders and community partners following an emergency or crisis event will improve future responses and serve as an opportunity to modify procedures, protocols, or plans to account for real-world outcomes during an event. There are many ways to conduct meaningful after-action reviews. Some suggested practices are:

- The after-action review should be conducted as soon as practicable after the event has ended—within one to two days if possible;
- The after-action review should include all participating or impacted organizations and parties. This may require multiple review sessions but, to the extent possible, all parties should participate together;
- The after-action review should be recorded, either by making detailed notes or on video, to memorialize individuals' reactions and responses and the record should be reviewed at a later time to determine valuable inputs;
- The review should last as long as is needed and should cover all aspects of the event, from pre-event activity through recovery;
- Lessons learned from the event should be incorporated into existing plans and new plans should be developed where gaps have been identified;
- Participants and personnel should be briefed on the outcomes of the after-action review; and
- An after-action report should be developed and published broadly amongst stakeholders, affected organizations and personnel. The lessons learned should also be shared openly with like organizations—other airports, for example—so that broader audiences can benefit from the experience.



Fort Lauderdale-Hollywood International Airport

Active Shooter Incident and Post-Event Response

January 6, 2017

After-Action Report

August 15, 2017

BROWARD COUNTY FLORIDA

Broward County Aviation Department
2200 SW 45th Street, Suite 101
Dania Beach, Florida 33312

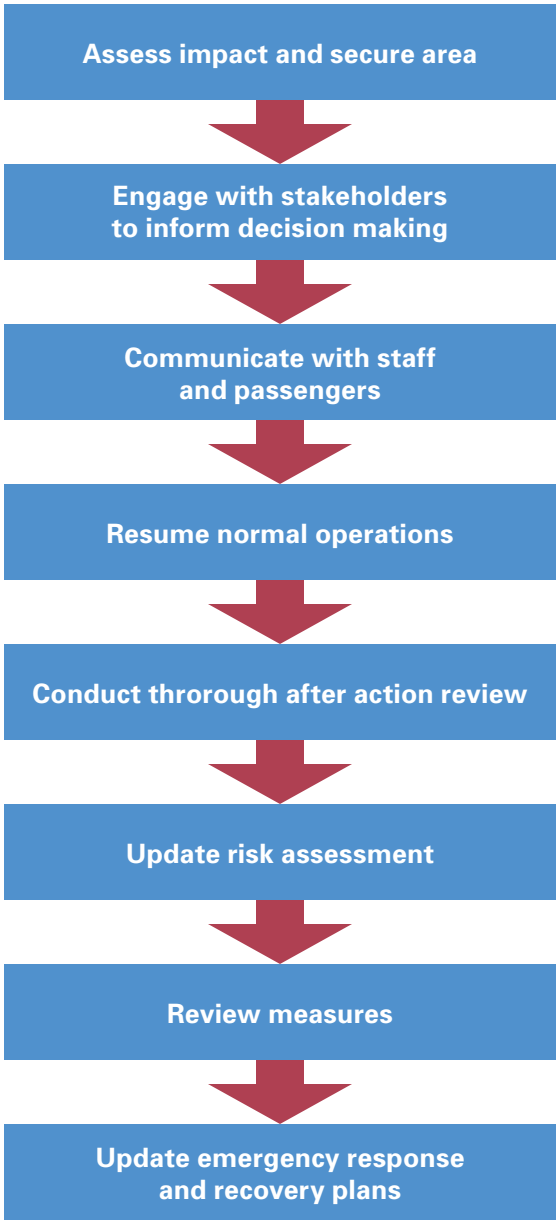
Example of after-action report following active shooter incident at Fort Lauderdale

6.7 Summary

Effective recovery operations depend on thorough planning that incorporates all-hazards scenarios which may impact an operation. Recovery, including resumption of complete or partial operations, focuses on fully restoring normal operations, repopulating public and secure areas while being mindful of ongoing investigatory and facilities requirements, and ensuring that staff members and other impacted individuals have confidence that they are safe.

Airport operators can expedite recovery timelines by incorporating redundant systems, capabilities and facilities into the planning efforts, exercising those systems on a regular and routine basis, and taking stock of lessons learned following any events that occur. Flexibility is also key and operators that are willing to explore alternate paths to recovery will ultimately benefit by achieving resumption of service and operations in a timelier and more effective way.

Following the recovery and review phase, lessons learned should be incorporated into emergency response plans. The risk assessment should also be reviewed and measures amended as necessary.



7 COMMUNICATION

7.1 Introduction

Due to the confidential nature of information on aviation security, the AVSEC community has traditionally tended to communicate very little. With the advance of public contribution to media reporting (including pictures/videos taken by cell phones) as well as the potential impact of social media (Twitter messages), speculation or incorrect information may reach the public at large without any quality control of the message being imposed and without prior consultation of authoritative sources. In the age of rapid international media coverage and social media advances, the risk in not engaging with media and with the public through social media is high, as airports may find themselves "running behind the message".

7.2 Communication during regular operations

New and more pro-active communication strategies may serve to both reassure the public about the security of the airport environment and have a deterrent effect. However, a balance must be struck regarding the protection of confidential information; it is important to note that in today's age of Internet, information intended for a small group is often available to all, and terrorists may make use of any information obtained online.

Equally, the mainstream media takes a great deal of interest in security for a variety of reasons:

- Rules and processes have an influence on travel behaviour;
- The perceived threat against civil aviation is based on a threat that resonates with the media and public;
- Many security regulations, processes and incidents are regarded as confidential and may therefore be more interesting to journalists wishing to reveal information;
- The public does not understand the reason behind certain security measures, nor why security measures differ from country to country; and
- Passengers may feel that their privacy is violated by certain security measures at the airport.

Airport authority communication strategies vary and are limited by different regulations regarding confidentiality of information. Communication strategies may also vary according to the travel habits of the general public.

Establishing a voice in regular communications is critical for the effectiveness of communication in potential crisis situations. Different types of communications may help to build a reputation as an official/authoritative source. Regular communication, for example of statistics or of other monthly/quarterly updates, provides a positive and neutral communication backdrop; and the public and media will become used to referring to this source for regular updates.

Airports may consider officially communicating new processes or technological advances, and explain why they are introducing them. Pro-active communication on such topics can create trust and allow the airport to lead the media discourse and inform passengers and the general public. Media events may also be created around new developments, as well as specific events that affect the airport and city it represents as a whole.

The engagement of media through round tables or information sessions may also help build the necessary relationship. In the event of a crisis, an established network of media and communications specialists allows for professional coverage of the crisis, within an established communications network. These journalists might be extremely valuable on an airport site during a crisis.

7.3 Communication in crisis mode

In a crisis, everyone wants to know everything as fast as possible, but there may be very little information to provide, or public authorities may prohibit anything from being said. However, every media vacuum is rapidly filled with speculation, so it is necessary to actively brief the media and the public to keep a certain level of control over the message.

It is critical to have a well-defined plan that is understood not only by those responsible for communication, but also by front-line staff who are likely to receive enquiries and by the senior management team.

7.3.1 Plan the team

Identifying the members of the team who will be responsible for communications during times of crisis and ensuring that roles are well understood is critical to ensuring that messages do not get out of control and come from multiple sources. Take the following steps:

- Plan for the communications team to be located in one room, preferably in the emergency operations centre or close to it;
- Designate a single channel of communication from individuals who are primary sources of incident information (e.g. operational/responder personnel) to the communication team;
- Identify additional resources that can be used (either from existing staff or via an agency) should the need arise;
- Plan enough resources to be available for three weeks following a crisis situation; and
- Identify clearly in easily accessible written procedures who will communicate with whom. Allocate responsibility for communications with:
  - Staff;
  - Press;
  - Public via social media and telephone;
  - Passengers via websites, apps and call centres;
  - Government agencies (public safety and security, local police, civil aviation authorities, ministry of transport);
  - Airlines; and
  - Third-party service providers and airport tenants.

7.3.2 Plan for public inquiries

Ensure that a call centre number is available for relatives of possible victims. Establish arrangements with an external call centre that can be stood up at short notice and define processes for communication with that call centre so that up-to-date messages are always provided.

Expect that enquiries may be received in multiple languages, so ensure that translation is available as needed.

7.3.3 Establish holding messages

Holding messages should be developed for all communication channels. In developing holding messages, airports should consider having them published on or circulated to:

- Their websites;
- Mainstream media;
- Twitter and Facebook;
- Airport mobile apps; and
- Public information services such as telephone enquiry lines.

The holding message should be simple and straightforward, acknowledging that there is an issue. An example might include a statement that "An incident has occurred at xyz airport and is currently under investigation. We will keep you informed of progress via our website."

If possible, provide a number that can be called for more information or direct people to the website for follow-up. Depending on the crisis, it may also be beneficial to ask people not to travel to the airport.

7.3.4 Backup website

The airport's website is a primary communication channel, and usually a major source of information about the airport and its daily operations. It is also one of the first places journalists, customers and others will look for information about an accident or major incident and how this might affect ongoing operations.

A crisis web page or backup site should be prepared that can be used immediately if a crisis occurs. This is a dedicated site which can be activated almost immediately (within minutes) after notification of a crisis and replaces the normal home page on the website. This page would normally be activated in the event of an incident with fatalities, although it may be appropriate in other circumstances, depending on the nature of the event and the degree of media/public interest (for example a massive systems failure which creates extensive disruption).

For less sensitive or critical events, a statement posted on the main website may be sufficient.

The backup site should be branded very simply, without any of the promotional material which normally

appears on the home page. It should display the latest statement on the situation, starting with the holding statement.

Customers should be able to click on a link to reach the standard home page so they can continue to access other information such as flight arrival times. However, any inappropriate images such as those illustrating retail promotions or resort information should be removed from the home page after an incident.

Other material which may be provided on the backup site includes:

- Background information on the airport company and its operations;
- A summary of the company's response to date; and
- Links to video of statements made by the CEO or other senior executives.

It is imperative that the backup site is not publically available during regular operations, even by direct unpublished link or via a search engine. Airport communications teams should liaise with their IT departments or web providers to ensure that agreed mechanisms are in place to activate the holding page immediately should it be needed.

7.3.5 Plan social media strategy

Social media channels to be used during a crisis should be identified (Twitter, Facebook, YouTube and others), depending on the airport's usual channels during regular operations. A strategy for how abusive comments will be dealt with should be agreed, as should a strategy for responding to specific questions. Video statements may be posted to YouTube and linked to from other channels—this should be agreed in advance between the senior management and communications teams.

7.3.6 Train and brief staff

All employees should be informed of the do's and don'ts regarding communication during a crisis:

- When answering telephones: identify the caller and questions; take a phone number for call-back;
- Forward all media requests to the communications team;
- Do not make media statements unless you are authorized to do so; and
- Do not voice personal opinions to the media, on social media or to friends.

Employees who are involved in the communications team should have clearly documented roles, including whom they should contact and when. Procedures for the development and authorization of messages should be pre-defined, as should an up-to-date list of contacts for media, airlines, airport stakeholders and government agencies.

Procedures should be established in cooperation with senior management, the airport's head of security, and relevant government and law-enforcement agencies. In times of crisis, emotions and tensions will be high, so having written procedures, clear roles and easily accessed contact lists will alleviate extra stress and confusion.

7.4 Communication in crisis mode

The balance between providing information and ensuring the confidentiality of sensitive information becomes especially important during a crisis.

7.4.1 Providing information

The airport communications team should give as much information as realistically possible in a timely manner. Bear in mind that a local message may have an effect on the international aviation system as a whole, if picked up by international media.

First steps in reacting to a crisis include:

- Activate the crisis communication plan (gather the communications team into an agreed location or find an alternative if the primary location is not safe);
- Gather information;
- Verify the information;
- Release a holding statement;
- Activate the airport's backup web site if necessary;
- Hold a press conference as soon as possible and always within two hours of the event happening;
- Provide a media update every two hours; and

- Offer help immediately and communicate it, and involve the airport's partners.

Internal communication:
- Employees should be informed before the general public is;
- Consider carefully the elements to be included in a written information statement to employees (as this may end up reaching outside sources inadvertently or through intent); and
- Explain clearly to employees what action they should take—if they should leave the airport or continue as usual, and how they can find out more information as the situation develops.

Coordination:
- Activate the crisis communications plan and ensure coordination with all stakeholders, if possible;
- Use the one-voice principle—all entities should be communicating the same message;
- Control media access to top management and specialists; and
- Make an initial agreement with press and media for regular press briefings to be held in a dedicated press room.

Communication with the press:
- Double-check the identity of the media representative (e.g. check the press ID, double-check the phone number, call the editorial office);
- Ask for a catalogue of questions. Do not reply to surprise questions;
- Ask about the planned rubric/context in which the information will be published;
- Enquire about other participants (do they have similar or different views?);
- Request a copy of the text/recording for archives;
- Only answer what you can answer; and
- Keep a record of media contacts (identify the reporters to whom you spoke, when you spoke to each and which information was provided; number press statements and photos).

Communication with relatives:
- Activate a specific call centre to deal with telephone enquiries.

7.4.2 Developing messages

For each audience, the key elements of the message and the best communication channels should be identified. When developing messages, a double-check by the communications and aviation security departments should ensure that confidential information is not included in the message and that the message is technically correct. Messages should also be cleared by local law-enforcement agencies depending on the situation and if there is an ongoing situation or investigation.

Message elements to consider when drafting the objective elements of message are the following:
- Who;
- What;
- When;
- Where; and
- Why.

Reference may also be made to:
- Applicable regulations;
- Approved security programmes;
- Stating the responsible entity for the process in question; and
- Making general reference to security processes in place.

When developing messages, the communications team should be sensitive to the different nationalities and cultures that may be involved. Messages should put people first—talk about people rather than facilities. Live appearances and videos should appear controlled but genuine.

7.4.3 Dealing with mainstream media

After an attack, the airport itself will become the focal point of media attention. Journalists will congregate in the terminal area attempting to find company spokespeople, eyewitnesses and possible victims. TV crews and photographers will also request access to the attack site, or a suitable vantage point. Depending on the circumstances, the airport itself may be temporarily closed or suffer serious disruption as a result of the attack, so it will need to communicate quickly with passengers and other airport users.

The airport operator will have an important role to play in dealing with the news media on-site and co-ordinating any press briefings or media access to the accident scene. If the airport has a media centre, this should become the location of media briefings by any of the parties involved. Where appropriate, joint briefings may be arranged which may involve the airport authority, emergency services, and/or the investigating body.

The airport should be prepared to respond to questions from journalists. Any statements or comments from the airport operator should focus on the following:

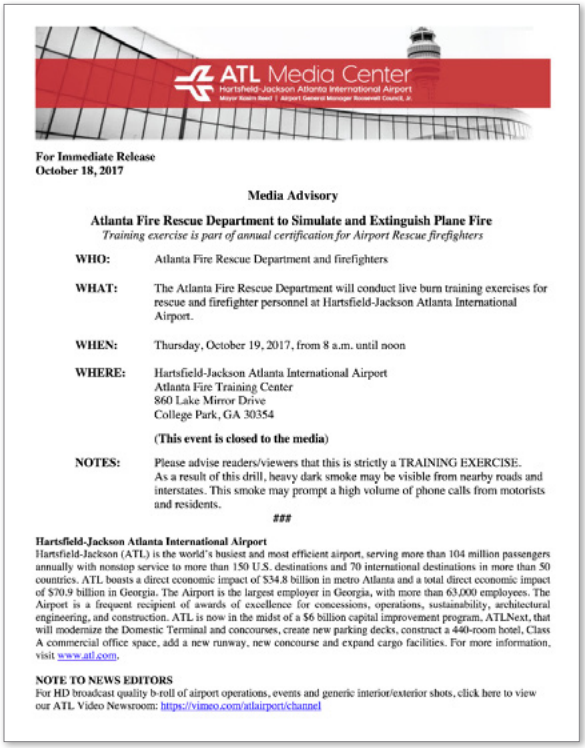
- Expressing concern for survivors and/or sympathy for victims and their loved ones;
- Providing factual information about the circumstances of the events;
- Discussing the progress of the search and rescue/recovery operation;
- Identifying the facilities and equipment which the airport continues to use during the recovery;
- Describing the impact on the ongoing operation of the airport; and
- Detailing actions the airport has taken to mitigate the impact to all tenants and to minimize passenger inconvenience.

All other questions should be directed to the emergency services or the investigating body.

7.4.4 Social media

An integrated, consistent and authentic communication response to an accident is essential, using all available channels to engage with the airport's internal and external stakeholders. Individuals within the management team who use social media personally should limit their comments to the approved messaging, which must remain authentic. Other employees should also be reminded of the company's social-media policy.

Monitoring online conversations ("listening") about the airport is an essential form of intelligence, particularly during a crisis, and will allow the airport to adapt its communication strategy and engage more effectively with key influencers as the story develops. There



ATL Media Center
Hartsfield-Jackson Atlanta International Airport

For Immediate Release
October 18, 2017

Media Advisory

Atlanta Fire Rescue Department to Simulate and Extinguish Plane Fire
Training exercise is part of annual certification for Airport Rescue firefighters

WHO: Atlanta Fire Rescue Department and firefighters

WHAT: The Atlanta Fire Rescue Department will conduct live burn training exercises for rescue and firefighter personnel at Hartsfield-Jackson Atlanta International Airport.

WHEN: Thursday, October 19, 2017, from 8 a.m. until noon

WHERE: Hartsfield-Jackson Atlanta International Airport
Atlanta Fire Training Center
860 Lake Mirror Drive
College Park, GA 30354

(This event is closed to the media)

NOTES: Please advise readers/viewers that this is strictly a TRAINING EXERCISE. As a result of this drill, heavy dark smoke may be visible from nearby roads and interstates. This smoke may prompt a high volume of phone calls from motorists and residents.

###

Hartsfield-Jackson Atlanta International Airport
Hartsfield-Jackson (ATL) is the world's busiest and most efficient airport, serving more than 104 million passengers annually with nonstop service to more than 150 U.S. destinations and 70 international destinations in more than 50 countries. ATL boosts a direct economic impact of $34.8 billion in metro Atlanta and a total direct economic impact of $70.9 billion in Georgia. The Airport is the largest employer in Georgia, with more than 63,000 employees. The Airport is a frequent recipient of awards of excellence for concessions, operations, sustainability, architectural engineering, and construction. ATL is now in the midst of a $6 billion capital improvement program, ATLNext, that will modernize the Domestic Terminal and concourses, create new parking decks, construct a 440-room hotel, Class A commercial office space, add a new runway, new concourse and expand cargo facilities. For more information, visit www.atl.com.

NOTE TO NEWS EDITORS
For HD broadcast quality b-roll of airport operations, events and generic interior/exterior shots, click here to view our ATL Video Newsroom: https://vimeo.com/atlairport/channel

Example of Press Release – Courtesy of Atlanta Airport

are numerous online tools which allow companies to monitor online conversations, to measure sentiment about particular issues, and to analyze the impact of the company's own social-media activities.

Twitter is the most widely used service, with millions of users posting short messages (tweets) to their online followers every day. Twitter has become a primary source of breaking news, particularly in fast-developing situations such as aviation-related incidents. A tweet from a survivor or eyewitness can reach tens of thousands of Twitter users around the world in minutes.

A Twitter feed should be established under regular operations and used for regular announcements and promotions. Hashtags (#) should be combined with keywords to "tag" the subject matter of a Twitter post—for example, "#(airportcode)". Tweets can be used to update followers on the latest information on the airport's response, for example, "#(airportcode) information center now open. Call 111 1111 1111 or visit link".

Posts should include links to more detailed sources of information—for example, statements posted on the company website.

Example of twitter post – Courtesy of Atlanta Airport

Facebook can also be treated as a primary communication channel after a serious incident. Any statements and information published on other channels should be posted to Facebook and updated at the same time. As with the airport's website, after an incident the cover photo and any colorful images on the airport's Facebook page should be reviewed and temporarily replaced by plain branding. Inappropriate or insensitive images should be removed.

Since users can post their own comments and refer to other sources of information, conversations on the Facebook page should be monitored and a policy established for responding to comments, or for correcting any misinformation or incorrect statements which are posted. Facebook can be a useful channel for engaging directly with customers in a crisis—for example, by responding to their questions in real time. Particular attention should be paid to posts by employees. If the post contravenes the company's social-media policy, it should be deleted or hidden.

The airport may choose to stream media briefings on Facebook Live, although you should consider whether to show only the CEO/senior executive statement or continue streaming during the question/answer session afterwards, during which the media may become hostile or persistently demand answers to questions that you cannot answer.

Even if the airport does not operate a dedicated YouTube channel, statements from the CEO or by other senior executives after an accident can be uploaded to YouTube. The video should be publicized by posting the link on the airport's website and on Twitter. When uploading videos to YouTube, choose the appropriate category and use keywords to describe the content. The tags will allow users to find the video via the YouTube search engine. As is the case with Facebook and other social-media sites, other users may post comments in response to anything posted on YouTube. The airport's communications team should monitor these comments and make a policy decision on whether to respond to any negative or misleading statements.

7.4.5 Communicating with other stakeholders: government, police, agencies and tenants

Numerous parties will be involved in the response to an attack. To a greater or lesser degree, all will face pressure to provide information to the news media and other parties, particularly in the immediate aftermath of the event. Depending on the circumstances, this may include the airline(s) involved, emergency services, the investigating body, government agencies and third-party contractors.

To avoid confusion and inconsistency, it is important that each party understands its role in the response, the kind of information it can legitimately provide, and the appropriate messaging to use.

As part emergency response planning, the airport will have activated its Emergency Coordination Centre (EOC). The alert is the first step in the initiation of any emergency. The purpose of the alert is to notify all agencies that are considered first responders to a potential, impending or actual emergency that has occurred at the airport.

Further information on emergency communication planning with other stakeholders can be found in Chapter 5.4 of this handbook

7.4.6 Coordination of messages with other stakeholders

During a time of crisis, there will be other stakeholders wishing to provide information outside of the airport's control. It is imperative that, as part of the emergency response plan, all messages that need broadcast be coordinated with the airport's emergency command team.

An incident of this nature affects multiple individuals and companies and there must be a united front when presenting solid messages to the public.

7.4.7 Communicating with next-of-kin and expectations

Depending on State legislation, notification of next of kin can be challenging. ICAO published its global Family Assistance Policy in 2013 to help guide states in ensuring that in cases of incidents, States can create regulations and policy on how next of kin need to be informed in cases of duress. Airports need to refer to any legislation in their respective State to determine the course of action and plan required to communicate to next-of-kin victims.

The expectations of accident survivors and families of victims is steadily increasing as a result of the activities of family advocates and associations (particularly those formed after previous accidents) and legal matters. Family groups have been willing to share experiences through the media and on the Internet, while legal entities are quick to offer themselves as alternative sources of information to the airline or investigating bodies.

7.5 Communication in recovery mode

7.5.1 Public messaging

A communications plan to keep the public informed while reinforcing positive messages should be put in place. Progress on when and how the airport will return to normal operations should be communicated, as well as assurances about the security processes which are in place.

7.5.2 Staff messaging

Like the public, the airport's staff should be kept apprised of any changes during the recovery phase after an incident. The communication team should have an individual who is in charge of airport staff communication so that this person ensures all statements issued externally are also provided to employees via internal communication channels such as blast emails, company/airport intranets, bulletin boards and any other social-media platforms authorized. This includes liaising with operational departments to ensure that front-line employees are provided with guidance on how to respond to customer enquiries.

Example of Staff Communication Poster – Courtesy of Montevideo Airport

8 SECURITY CULTURE

8.1 Developing a positive security culture

A good security culture in an organization is an essential component of a protective security regime, which supports and maintains a risk-resilient organization that helps to mitigate against both insider threats and external threats. Security culture is the set of values, shared by everyone in an organization, which determine how people are expected to think about and approach security and having a strong security culture is essential in ensuring that the security regime which exists to protect an airport's personnel and visitors is effective.

Among the benefits of an effective security culture are that:

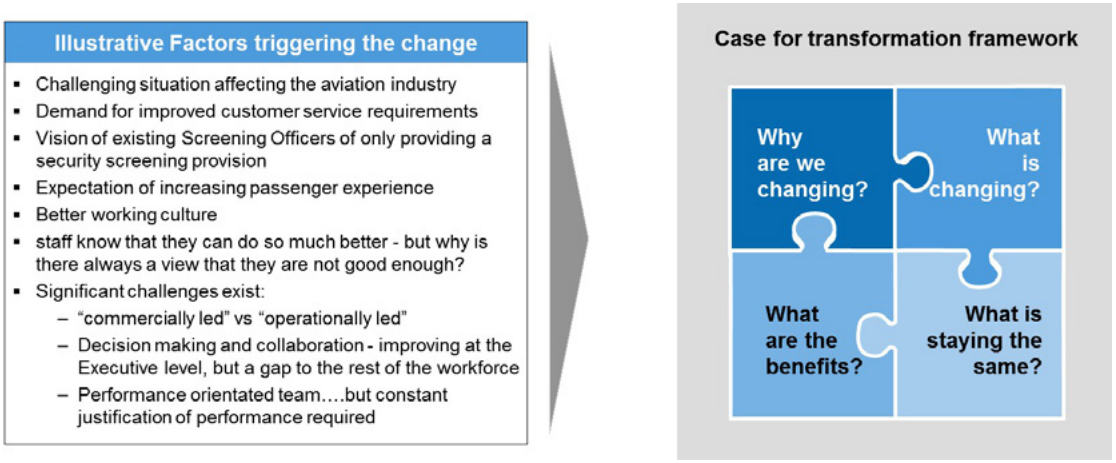
- Employees are engaged with, and take responsibility for, security issues;
- Levels of compliance with protective security measures increase;
- The risk of security incidents and breaches is reduced by encouraging employees to think and act in more security-conscious ways; and
- Employees are more likely to report behaviours and activities of concern.

Elements of a strong security culture	
LEADERSHIP	• Security is written in goals and values of organization • Management are receptive to feedback • Management visibly implement corrective measures and lessons learnt • Management support security training (time and resources)
AWARENESS	• Staff have a good awareness of risks • Staff have a strong alertness to threats • Staff have understanding of their own role in security • Security is second nature
RESPONSIBILITY	• Staff are motivated to perform well and rewarded fairly • Security comes first, even when under pressure • There is a willingness to accept responsibility • There is a willingness to challenge others and be challenged • Staff employ critical thinking and proactiveness
TRAINING	• All staff have an understanding of correct processes and procedures • All staff are given awareness training, including those employed by the airport and other on-airport workers
COMMUNICATION	• Management often talk to staff about security • Security is publicised, through posters, newsletters and brochures • There is a clear policy or code of practice that is visibly displayed • There is a non-punitive reporting culture

8.2 Managing the change

In order to implement change in the organization successfully, a clearly defined communication plan must be created alongside a strong change-management program.

A successful change-management program is one that ensures that people understand what is changing and why; that they feel accountable; that they have the necessary skills and knowledge; and that they are incentivized to work in the new way.



Evidence shows that change activities are driven by a set of defined people outcomes

	Outcomes	What do they mean?	What risks are addressed?
1	People understand the change	▪ People understand what is changing ▪ People understand the benefits of the change and why it needs to happen	Rumour, stress, absence, decreased productivity
2	People accept and feel ownership of the change	▪ People feel engaged in and accountable for the change - not that it is being done 'to' them	Disengagement, attrition, low participation / investment in achieving outcomes
3	Our people are enabled to lead the change	▪ People at all levels are committed to making the change work ▪ Leaders are accountable for driving and delivering the change	Lack of commitment, failure to deliver the change and achieve benefits
4	People have the knowledge, skills and behaviours needed to work in the new way	▪ People have the necessary knowledge and technical / management skills to work in the new way ▪ People exhibit the behaviours and mindset that will enable them to operate effectively in the new environment	Failure to fully adopt and deliver new responsibilities and ways of working
5	People consistently work in the new way and it feels normal to them	▪ New ways of working are "the way we do things" ▪ People are able to spot capability gaps and coach others when required ▪ People are incentivised to continue working in the new way	Gaps in workforce capability Conflicting guidance from supporting HR systems including performance management

Change management—Courtesy of McClumpha Associates

8.3 Training, awareness and motivation

Vigilant security behaviour demonstrates a vigilant, attentive and proactive organization to staff members, to the travelling public and to hostile individuals. It demonstrates that routine surveillance measures such as CCTV and the presence of security staff are not the only measures in place: alert employees are just as likely to spot suspicious activity and report it.

A highly motivated workforce can have very powerful influences on positive security behaviours. Unless employees understand the threats that they and their organization face, they will not be inclined to change how they act. Educating employees about the nature of the threats, their potential impact and the role all employees can play in countering the threats is therefore critical.

Training for all employees should include an overview of terrorist threats; regulations; the roles and responsibilities of all staff members; the security measures in place at the airport; and the resources available. Staff members should be provided with real-life examples of relevant poor security behaviours and their consequences. For example, prepare an intranet story about a security breach at an airport, the impact of the breach and how it could have been avoided. Conversely, examples of good security behaviours should be publicized and the resulting successful impacts detailed.

8.4 Responsibility

The role of all staff members in providing security should be emphasized. In addition to training and communication, airports may wish to consider how to write compliance measures into their security policies. This should involve the human resources department in a discussion about how to introduce vigilant security behaviours into staff induction, appraisals and personal-development plans.

8.5 Creating a project plan and communications strategy

Changing security behaviour requires a clear vision and a coordinated strategy to ensure that interventions are consistent, practical and meaningful.

The following steps are recommended to prepare and run a security behavior-change campaign:

- Step 1. Gaining the support of senior management and internal communications colleagues;
- Step 2. Bringing together a team to deliver the campaign;
- Step 3. Developing an overarching strategy; and
- Step 4. Developing and applying a project plan.

The first step is to gain buy-in from senior management. Support from the internal communications team is also critical to success. These colleagues will understand the best ways of communicating with employees and can suggest various lines of communication (e.g., staff newsletters, intranet etc). The aim is to make both senior managers and internal communications personnel aware of the threat, the aims and the objectives of the campaign and why it is essential to run the campaign.

Second, one leader for the campaign should be appointed to be its visible champion, to take ultimate responsibility for its delivery and, if required, report on progress to the board or CEO. Management and communications specialists may express concern about causing alarm amongst airport employees. It can be helpful to explain that while underlining risks, the campaign will also provide positive messages about the impact of a workforce with a unified approach to security. It is also useful to invite help and involvement in pitching communications. Research has found that employees overwhelmingly respond positively to campaigns of this nature. It is recommended that the project team includes a project manager, a senior management champion, the airport security manager and a communications-team member.

One of the first outputs from the campaign team should be a simple, agreed strategy from which a project plan can be developed. This does not need to be complicated. Indeed, it should be simple and clear. To develop a strategy, address the following questions:

- Why are is the airport undertaking a campaign? What is it you want to achieve? What is your vision?
- What are existing staff behaviours, good and bad, in terms of vigilance and reporting?

- How aware are staff members of the threat to them and/or the organization?
- Do the employees know what suspicious activity is and how to report this immediately?
- What are the potential barriers or facilitators to employees undertaking the behaviours you want—e.g., their being uncertain as to what will happen to their reports, a belief their reports not being taken seriously, there being no control room number on the staff intranet, etc.?
- What specific behaviours do you want to see as a result of improving awareness of the need for employee vigilance and how might you measure this?
- What are the delivery mechanisms? How do staff like to receive information—e.g., by newsletter, intranet, briefings, or special security-awareness events?
- Do you have contact with credible experts whom you can bring in to support and endorse your campaign—e.g., local police or the security regulator?

It is important that staff members who already display good behaviour are acknowledged for it in the campaign and encouraged to continue displaying such behaviour. The fourth step is to create a project plan with clearly defined timelines, deliverables and responsibilities. An example of a project, offering defined steps to develop staff motivation, is provided below.

Example of project—Steps towards implementing a security culture program

Each step should be broken down into tasks, assigned a start and end date and the person responsible for its implementation identified. This will enable the project to be tracked and managed effectively.

Step/Task	Start	End	Person responsible	Status
Incentives program				
Define incentives				
Agree budgets				
Sign off human resources and senior management				
Develop communication materials				
Amend annual performance review				
Communicate to staff				

Example extract from project plan

8.6 Communication tools

Some of the tools that might be included in a communications campaign are:

CEO's weekly newsletter:
- Outline the threat and how staff behaviour can aid protective security;
- Emphasize the role that staff members have to play; and
- Publish the contact number for reporting security concerns.

Intranet article on 'Thinking like the enemy':
- Explain what is meant by hostile reconnaissance and describe the effects that staff behaviour can have on those conducting it; and
- Invite a credible external expert to highlight the deterrence effect of staff behaviours.

Security manager's blog or article:
- Describe any bad security behaviours seen by security and explain why they are bad. Detail what good behaviours are. Indicate when the security measures are strong but explain that staff can help enhance them by being aware of their own behaviour, being vigilant and reporting in. Describe what happens to reports from staff members, providing real examples and detailing outcomes;
- Emphasise that security officers welcome all assistance from staff members and will treat any report from a staff member with due respect; and
- Highlight any reward campaign and confidential reporting mechanisms.

Security awareness event:
- Showcase all protective security measures in place—e.g., offer visits to the control room, allow staff meet the patrol dogs, etc.; and

- Have security officers endorse the campaign and convey to staff members that they have a key role to play in assisting site security; have security officers say they welcome reports, etc.

Posters:
- Detail what suspicious activity to look out for; and
- Provide a phone number on the poster, along with a reminder to report suspicious activity immediately.

Wallet cards:
- Provide a reminder of what to look out for and to report in immediately; and
- Provide a phone number to call to facilitate reports when off-site.

Staff survey:
- Conduct short interviews with staff members to ascertain if they have understood and accepted key messages, find out how they felt about the campaign and establish whether they have changed their behaviours as a result.

8.7 Making behaviours easy to adopt

To encourage employees to practice vigilant security behaviours, the behaviours must be easy to adopt.

This means providing simple steps that employees can take to improve personal security behaviours, and ensuring that they know what to look for and exactly how to report suspicious behaviours.

8.7.1 Giving an impression of vigilance

Vigilance on the part of staff members can be conveyed, for example, by enquiring "Can I help you?" if someone appears out of place or is acting differently. The prospect of staff engaging in a customer-friendly way is a strong deterrent for a hostile conducting reconnaissance. A simple "Can I help you?" conveys that staff members are not only good at spotting people out of place but, critically, will do something about it by approaching them. Encourage employees to be customer-friendly and helpful; if they see someone loitering or perhaps in a place where the person shouldn't be, they can enquire if the person needs help, before reporting in to security if they feel the person's behaviour was suspicious.

8.7.2 Reminders of suspicious behaviors

An easily accessed reminder list of suspicious activities is really useful. Such activities include:

- Loitering around or near restricted areas;
- Taking photographs of staff or security features of the building;
- Someone taking an interest in staff/vehicle movements;
- Inappropriate approaches to any staff member;
- Someone following someone else (including staff members) unobtrusively;
- Packages/bags being left unattended;
- Suspicious vehicle activity in close proximity to the terminal or the airport perimeter; and
- Anything you feel isn't right.

8.7.3 Clear and easy instructions

The instructions for reporting must be clear and be widely communicated throughout the organisation. Consider giving all staff members a wallet card featuring the reporting number, so that they can carry the card around with them when they are on-site and off-site.

Large banner posters in entrances and exits to staff areas will remind staff, at the point that they enter or leave, to be vigilant and report suspicious activity.

Posters can easily be tailored to the airport's own branding and house style, its photography resources and its call to action. Although some organisations prefer to use their own house colours for posters advising the need for vigilance, research has shown that a red background tends to command attention in a security environment. To keep the posters fresh, it is recommended that they are refreshed every few months. This will improve the uptake of the messaging.

SECURITY CULTURE

Security is everyone's responsibility

Together, we've got it covered.

Introduction

Do you know what suspicious activity looks like? Do you know what to do if you see something out of the ordinary? Remember, being seen to be vigilant and ready to engage with the public can also help deter criminals.

Police response (the 5 Ws)

- What is it?
- Where is it?
- When was it found?
- Why is it suspicious?
- Who are the witnesses?

HOT protocol (unattended items)

H – Hidden
Not in general view and may have deliberately been positioned in a discrete area.

O – Obvious
This is when the item is obviously suspicious, signs of tape, wiring, batteries etc.

T – Typical
Not typical of the normal, everyday situation; out of the ordinary.

If in doubt, DON'T ignore it.
Tell your supervisor.
Call your control room.
IMMEDIATELY on XXXX XXXXX

Together, we've got it covered.

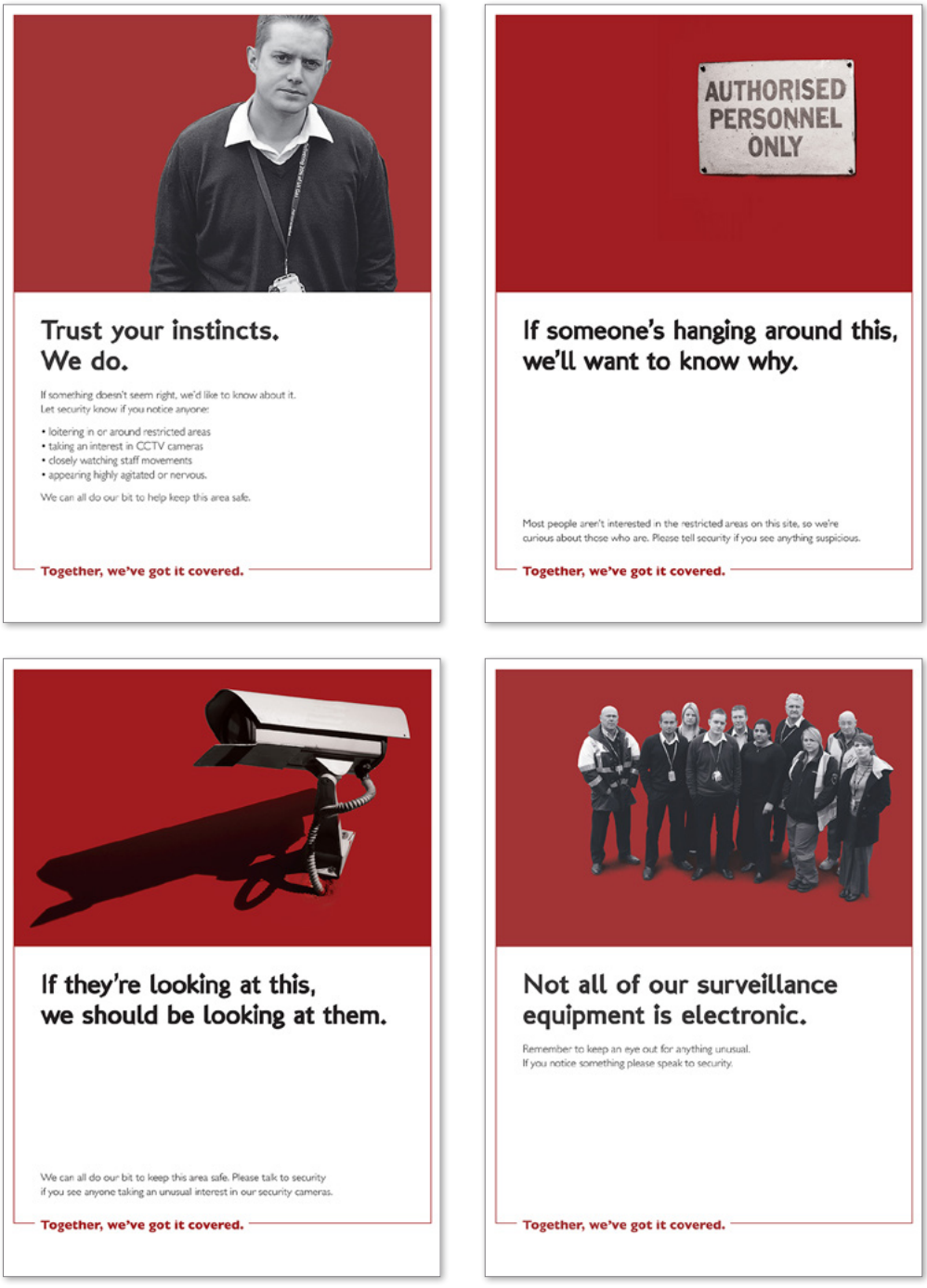
Suspicious activity

Always be vigilant for people:

- Hanging in or around restricted areas
- Taking an interest in CCTV cameras
- Closely watching staff movements
- Appearing highly agitated or nervous

You know what's normal. Trust your instincts. Report any suspicions IMMEDIATELY. In doing so you are helping to ensure your safety and the safety of those around you. Don't forget the power of a simple 'Can I help you?'

Example of wallet card (CPNI)



Examples of awareness posters (CPNI)[5]

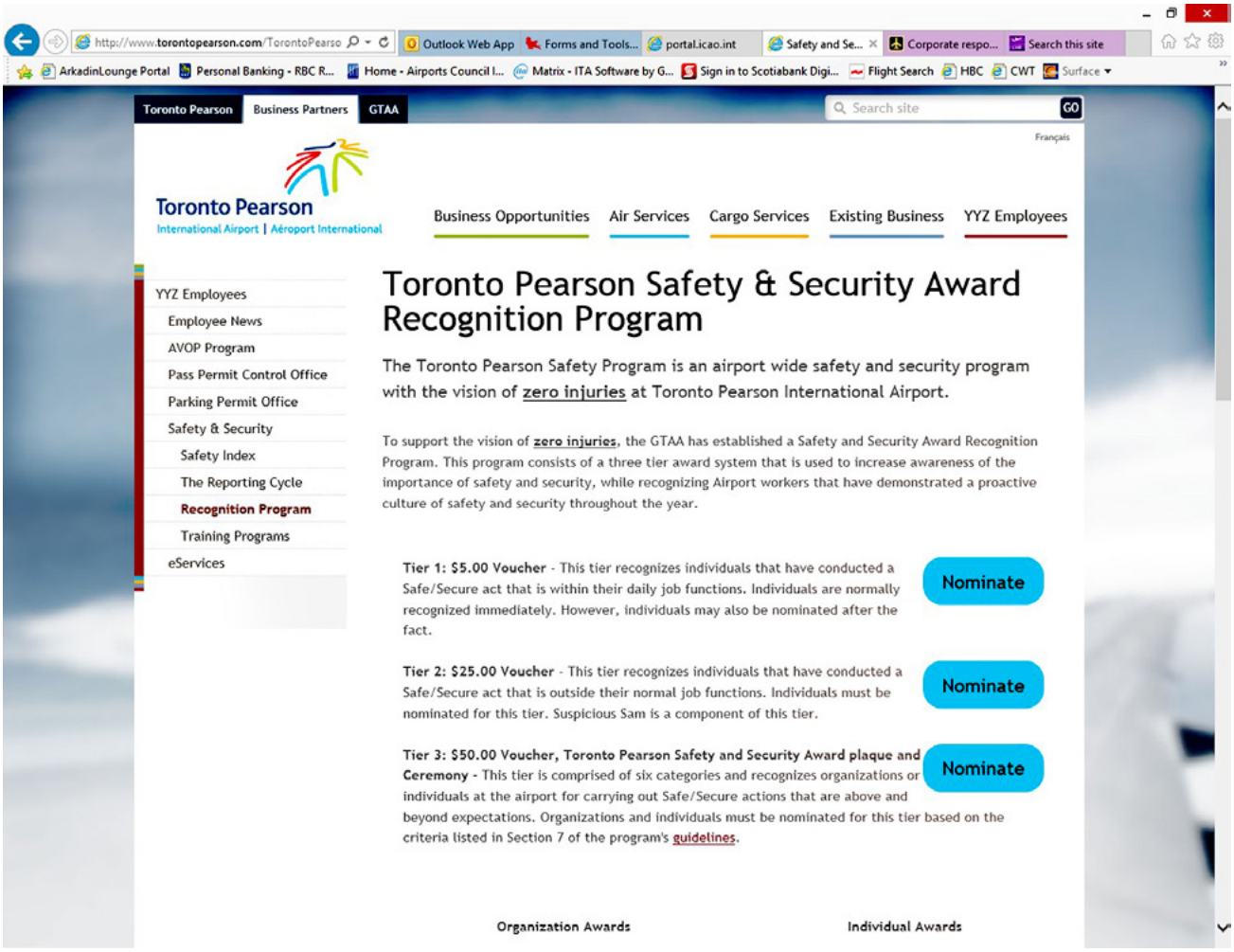
[5] Further resources may be found at https://www.cpni.gov.uk/security-awareness-campaigns

8.7.4 Reporting and rewards programs

It is important that every staff member knows that his/her report has been taken seriously. It is equally important that each report is analyzed and that follow-through action is taken on it, not only with immediate action if a risk or vulnerability has been identified but also with a root-cause analysis so that future issues can be prevented or mitigated if possible.

Toronto Pearson's reporting cycle

Additionally, the airport may wish to offer employees rewards for good security behaviours such as reporting of suspicious items or behaviours. This has to be carefully managed so that false reporting is not encouraged and security does not become a competition between staff members. One example program (below) offers tiered awards for proactive acts within a job function, for safety and security behaviour outside of the normal job role and for actions that are above and beyond expectations.



Toronto Pearson's safety and security award recognition program

8.7.5 Engaging the public

By engaging the travelling public in promoting airport security, an enormous additional security resource can be generated. Encouraging members of the public to report suspicious behaviour or unattended items, for example, can act as both detection and deterrence. Of course, this requires that sufficient resources be made available to act on reports being made. Responsibilities need to be clearly defined—for example, suspicious behaviour might be reported to the airport security staff or to the local police, depending on what has been agreed.

In asking passengers to remain vigilant, posters and public service announcements can both be considered. Any measures put in place should provide a balance between asking passengers to be aware and reassuring them that the airport is safe and secure.

Airport watch – Courtesy of Adelaide International Airport

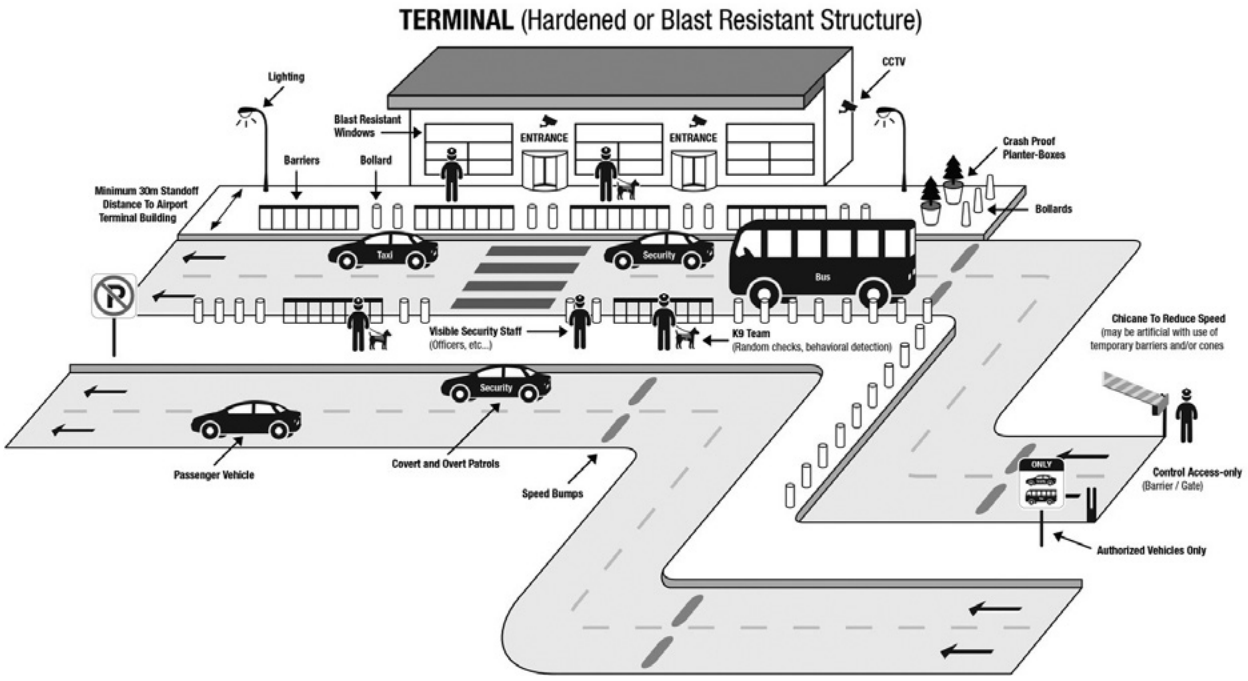
9 BUILDING DESIGN

9.1 Design process

Many of today's security risks are a direct result of security being 'bolted-on', not being considered or being considered too late in the design phase to be included or effective. This can result in:

- Missed opportunities to design out risks;
- Retrofitting of measures that can be more expensive and/or less effective than a designed-in measure; and
- Ancillary measures conflicting with other design and business objectives, for example passenger experience, aesthetics and wayfinding.

Using risk-based security by design requires security to be considered in all infrastructure design even if the project's scope does not have security content. An example is the surface-transport strategy and design. In the face of it, road design does not have any security scope. But involvement of security early and the conduct of the risk assessment might identify that the length of the road will assist a penetrative vehicle-borne improvised explosive device VBIED attack. If the design is adopted, hostile vehicle mitigation (HVM) and blast resilience will need to be retrofitted to a number of buildings in the vicinity. Identifying this early may result in the road being redesigned at nominal additional cost. The security risk that was designed-in with the road being straight and long has been negated and along with that so has the additional capital cost for HVM and blast resilience retrofitting.



ICAO Doc8973 Landside Security Guidance

When designing infrastructure (new or retrofit), future-proofing should be considered in order to avoid future deployment being less effective. This might involve:

- Quarantining space for additional equipment or processes, e.g. creating landscaping that allows the opening of lay-by lanes for vehicle searching;

- Building redundancy into IT systems to accommodate future deployment of equipment, e.g. CCTV;
- Record-keeping of infrastructure and systems
- Building in flexibility to allow assets to be used for alternative purposes, e.g. using a car park as a pick-up and drop-off point if the forecourt road is closed; and
- Designing processes and communications that change the behaviour of airport users.

The policy, including roles and responsibilities, for the reduction or withdrawal of measures as levels of threat come down must be established, agreed and communicated. This avoids confusion that may result in measures being withdrawn too soon (a security risk), measures being deployed unnecessarily (creating resource wastage and facilitation obstruction) and invalidation of insurance.

9.2 Security through environmental design

Security outcomes through environmental design are achieved by:

- Designing out features that increase the likelihood of an attack (such as the attractiveness of the target and the vulnerabilities it offers); and/or
- Reducing the consequences of an attack.

The appeal of environmental design is that it does not require further capital or operating expenditure to maintain its security-effectiveness and can reduce the need for security measures. The following example, on the right, illustrates this.

Establishment of a forecourt with landscaping that incorporates hostile-vehicle mitigation measures—e.g. a bund—provides a stand-off distance that reduces the risk through, first, reducing the consequence of a vehicle borne improvised explosive device (VBIED); and second, reduces the attractiveness of the terminal as a VBIED attack target. The stand-off distance is established; it does not require ongoing maintenance or operations to maintain its risk-reduction capability. Furthermore, the forecourt can be incorporated into the public realm design, further strengthening the business case of the security outcome (photo courtesy of Adelaide International Airport).

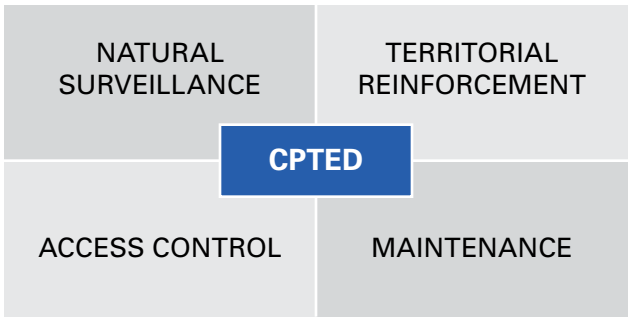
The use of environmental design to accommodate security measures can improve the effectiveness of security measures and in some cases reduce the amount and/or cost of those measures. The following example, on the right, illustrates this.

The ceiling fixtures and architectural design of the passenger ferry terminal take into account the need for lighting and CCTV for security purposes. Designing the fixtures in up-front avoids the need for retrofitting fixtures and provides integrated ICT. The architectural design reduces the number of lighting and camera fixtures as the CCTV can work more effectively without coverage interference.

9.3 Crime prevention through environmental design

Crime Prevention through Environmental Design (CPTED) is the use of design and space-management principles in order to manipulate human behaviour. It is a crime-prevention strategy based on proper planning, design and structure of cities, neighbourhoods, precincts or individual sites to create the effective use of the built environment which can lead to a reduction in the fear and incidence of crime, as well as an improvement in quality of life.

The design of a particular space has to ensure that the intended activity can function properly, as well as directly supporting the control of behaviour, in order to reduce the opportunity for crime. The design of the precinct should strive to incorporate the four overlaying CPTED strategies as illustrated below.



Four strategies of crime prevention through environmental design

Adeleide Airport's forecourt demonstrates good environmental design and an attractive environment for passengers which incorporates many security features (Photo courtesy of Adelaide International Airport)

9.4 Landscaping

As well as improving the environment and the customer experience, correctly sited and designed landscaping features are beneficial to aviation security—for example, by preventing hostile vehicle encroachment and/or impact. To maximize the security benefit, landscaping features designed for hostile vehicle mitigation must be constructed from suitable granular material. The use of loose rocks or rubble is to be avoided as they add considerably to the detrimental secondary effects of an explosion. No landscaping should be sited as to provide a 'ramp' possibility for vehicular penetration.

Planters can act as a feasible and cost-effective barrier. When planted, the plants must be tightly formed and have no excessive foliage and each plant should be no more than 300mm from base to top, in order to restrict the opportunity to hide a threat item within the planting.

Planter installation – Courtesy of Atlanta Airport

Trees should not be considered as providing a robust barrier, unless they have been evaluated by a subject-matter expert and are of sufficient diameter and depth. Trees should also not be planted within the 3-metre clear zone of the restricted area boundary. Features such as rivers, streams, roads or service tunnels which pass under, over or through terminals or cross the airside/landside boundary should be assessed and secured.

9.5 Blast mitigation

The performance criteria for any blast-mitigation enhancement should aim to meet quantitative limits or objectives set out within the security strategy or risk assessment. Common performance criteria for blast enhancements include the following:

- Life safety;
- Protection of critical assets; and
- Business continuity/recovery.

Blast mitigation typically aims to enhance structural elements to prevent damage and/or collapse and enhance non-structural elements against fragmentation to prevent injury (a secondary goal). It is difficult to mitigate against the primary fragmentation contained within the device itself.

Simplistically, a blast-mitigating structural element is designed by calculating the blast load on that element and by undertaking structural dynamic analysis to achieve a specified damage tolerance or response. Key concerns regarding the performance of a structural or façade element include collapse of the structure, the degree of secondary fragmentation (fragmentation from the structure itself) created, glazing (and glass fragmentation) performance, maintaining the building envelope and repairing damage. For these reasons, structural elements are generally defined into the following categories:

Primary structural component: A structural member whose failure results in collapse of other supported members and potentially the loss of the building's stability. These elements—e.g. a structural column, floor beams, trusses and load-bearing walls—have the most stringent design criteria, as they are the most critical elements and their failure can result in significant consequences. Loss of these elements also relates to disproportionate collapse. This is discussed in further detail later in this handbook.

Secondary structural component: A structural member—e.g., secondary beams, floor slab—whose failure results in failure of the member itself.

Non-structural component: A component that does not have a structural support function—e.g., a balustrade, façade element, non-load bearing wall etc. These elements typically do not require blast resilience, unless their failure may pose significant risk to life safety.

Glazing: Glass contained within the building façade, or within the internal space of the building. The performance of these elements directly relates to fragmentation and maintaining the building envelope.

Blast strategies to design against vehicle-borne IEDs and packaged devices will vary and should be determined in consultation with blast-engineering specialists.

9.5.1 Building stand-off/Set-back

Creating separation between the source of an explosion and the asset to be protected in a blast event is an effective means of minimising damage to the structure and potential human injuries/fatalities. Increasing distance from the point of detonation produces an exponential decrease in blast overpressure and therefore a reduction in fragmentation velocities.

The separation can be created using two approaches:

Set-back—This involves the use of landscaping, master planning and street furniture to "push" vehicles away from buildings and people. These measures would not prevent a deliberate ramming attack (although they may deflect or hinder a vehicle) but do allow suspicious vehicles to be quickly identified.

Stand-off—This is created via the use of impact-rated vehicle barriers that will stop a hostile vehicle at the defined perimeter. A stand-off does not need to remain permanent: operable and temporary barriers can be deployed to create a temporary stand-off at specific times when it is required.

Creating a stand-off and set-back within existing infrastructure assets cannot necessarily be easily achieved and the technique should be used in conjunction with other blast-mitigating enhancements, such as structural or façade enhancements to the building. Key considerations on the designation of capital to achieve blast protection are the costs of land and of perimeter protection.

A stand-off is generally built and secured by installing impact-rated bollards It is, however, critical that the barrier line is appropriate, proportionate and effective to the asset or people it is protecting.

Impact rated bollards – Courtesy of Adelaide Airport

Where blast threats are identified in the risk assessment, enhancements to the building's façade and structure provide a commonly identified mitigation measure.

Blast-loading of structures is not commonly considered by building designers. Unless specifically stated in their brief, engineers and architects will not design to resist blast loads. If the blast threat is present this approach may be considered.

The four primary factors that influence the performance of structures under blast loads are:

- The intensity of the blast loads (how large the charge is and where it is located);
- The desired level of performance (e.g. life safety, economic repair, immediate occupancy);
- Materials used in the structure (how strong they are and how hazardous they are when they fail); and
- The type of construction used (how the blast loads are resisted and absorbed by the building).

Additionally, not all levels of blast resistance are alike—the higher the loads and level of performance required, the more extensive (and expensive) the blast enhancements will need to be.

9.5.2 Managing blast enhancements

Blast enhancements to new and existing structures can result in significant costs if not managed appropriately. This section discusses how to manage blast enhancements to limit potential costs.

New buildings

If a new terminal building is being constructed then relevant national and international guidance should be followed as far as possible. This includes:

- Providing a stand-off to unscreened vehicles (the distance should be proportionate to the threat, as determined by a threat assessment);
- Ensuring that a robust blast-resistant façade system is installed;
- Designing the structure to withstand blast damage without suffering disproportionate collapse; and
- Using fixtures and fittings that limit the formation of hazardous debris.

Whenever these enhancements cannot be implemented, facility operators should consider how operational security measures can be implemented to reduce the building's potential vulnerability to blast.

Existing buildings

Existing buildings may not have been designed with blast in mind and may be vulnerable to blast attacks. However, the costs of enhancing the building to a standard equivalent to that of a new-build structure may be prohibitive. In such cases, the operator should look to reduce the building's vulnerability to blast as far as reasonably practicable. The process involves:

- Undertaking a blast-vulnerability assessment to identify the consequences of an explosion and the largest vulnerabilities;
- Developing measures to reduce vulnerabilities as far as reasonably practicable; This may include installing HVM to increase the stand-off to critical areas;
- Revising internal building layouts to reduce the number of persons exposed to the blast threat;
- Minor structural/façade enhancements (e.g. adding anti-shatter films to existing monolithic glazing);
- Reducing the attractiveness of the target; and
- Using operational-security measures to reduce the potential vulnerability to blast.

Refurbished buildings

When refurbishing a building, the intention should be to introduce blast enhancements to bring the performance of the structure and façade into line with new-build structures.

Achieving the same performance as a new-build structure may not be possible for reasons such as:

- The stand-off cannot be increased owing to site constraints;
- The existing structure cannot support a blast-enhanced façade; and
- Structural enhancements are not included within the scope of the refurbishments.

As with existing buildings, vulnerabilities should be reduced as far as reasonably practicable.

Example

In this example an existing 1960s airport terminal building is considered. A large vehicle drop-off area was incorporated in the original design to allow vehicles to stop adjacent to the terminal. No blast enhancements were considered in the original design.

Following a revised threat assessment, the risk of a potential vehicle-borne improvised explosive device being used against the terminal is identified. Impact-rated vehicle security barriers are proposed to provide a stand-off to the terminal and to prevent ramming attacks.

Where possible a 30m stand-off distance is provided, but in order to retain some drop-off capability the 30m stand-off is not provided everywhere. A level of residual risk remains so police patrol the drop-off area and ensure vehicles are not left unattended.

Later an extension to the terminal building is constructed. Owing to the constrained site, the desired 30m of stand-off cannot be achieved. Instead, the new structure is enhanced to withstand blast loads.

Designing the façade of the extension to withstand a vehicle-borne improvised explosive device detonated at the shortest distance from the building (approximately 5m) is not practicable or cost-effective. Instead, the façade is designed to withstand a detonation at 30m. The residual risk of a device located closer to the terminal than 30m is managed by the previously provided police patrols.

The extension to the existing terminal incorporates a blast-resistant façade and structural enhancements.

Finally, the existing terminal building façade is refurbished. As part of the refurbishment, the new façade is designed to withstand the same load as the terminal extension façade. The existing terminal structure is not refurbished, but the blast engineer assesses the structure to verify that it is capable of supporting the enhanced façade.

The refurbished façade to the existing terminal is enhanced to the same level as the newer terminal extension.

In this example, blast protection is enhanced in line with the works and site constraints that are present.

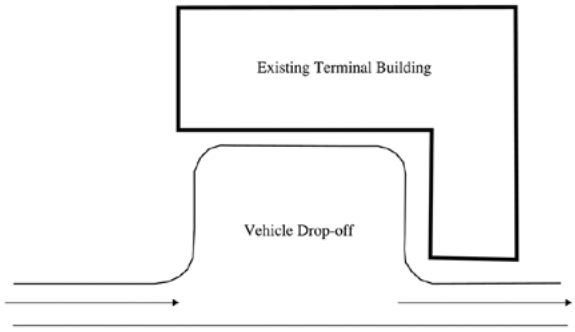


Figure 3: Existing terminal building and drop-off layout

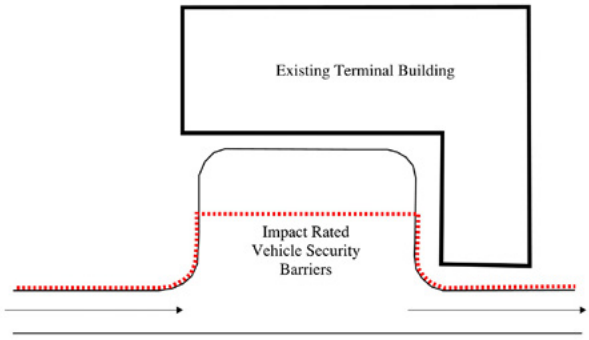


Figure 4: Layout of retrofitted vehicle security barriers (stand-off ranges from 25m to 7m)

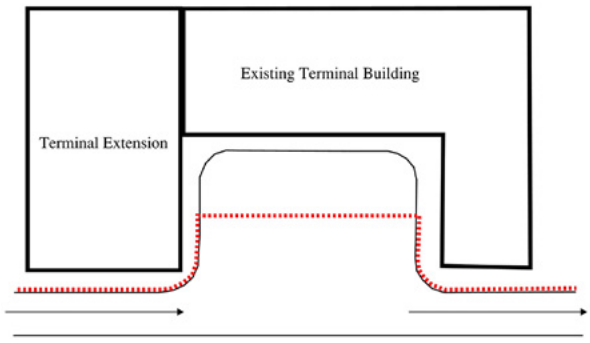


Figure 5: Extension to existing terminal

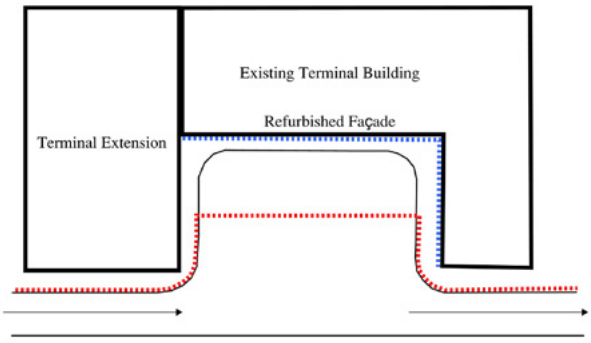


Figure 6: Refurbished facade

9.5.3 Design against progressive or disproportionate collapse

As part of the overall blast-resilience of the airport terminal, structural elements directly exposed to blast overpressures should be analysed and enhanced accordingly. The level of enhancement will depend on the criticality of the structural element and whether failure of this element will result in disproportionate or progressive collapse.

In the event of a blast scenario, a structure responds according to its robustness and a number of key different factors affect this. These include:

- Structural material;
- Framing layout;
- Framing connectivity;
- Ability to transfer load through alternative paths; and
- Primary element resilience.

If any of these factors are lacking then the structure could suffer what is known as disproportionate or progressive collapse. This would be catastrophic to the damage suffered by the building in question.

A disproportionate collapse is one that suffers damage which is in excess of that defined as tolerable. The definition of what is deemed tolerable is set down in either national guidelines or by specific airport owner/operator requirements.

The acceptable levels of damage stipulated in national guidelines are generally based on accidental actions (gas explosions, etc.) and therefore when reviewing damage based on a malicious event, the severity of the action needs to be taken into account. This can be undertaken by blast-engineering specialists.

A progressive collapse is one where damage to a structure causes the gravitational load to transfer through an alternative path. This alternative path in turn overloads the support mechanism and causes collapse. This failure mechanism can propagate throughout the structure and global collapse will result when every load path has gone. This was witnessed in the aftermath of the Oklahoma City bombing in 1995.

9.5.4 Glazing

The façade of the terminal building is a key design consideration for the overall blast-resilience of the building. If poorly designed against blast, the façade can break into high-velocity, highly hazardous fragments which can cause widespread injury and fatalities to people inside the terminal building.

Alternatively, if the façade is designed appropriately, it can act as a building envelope that does not produce highly hazardous fragments and prevents the influx of blast overpressures into the building's internal space. Selection of the façade glazing should be performed in consultation with blast-engineering specialists.

Progressive collapse witnessed in the aftermath of the Oklahoma City bombing in 1995

9.6 Site transport planning

In addition to stand-off/set-back distances associated with car parks, redundancy should be designed so that car parks can be used as thoroughfares in periods of heightened threat. For example, should lanes adjacent to the terminal frontage be closed during a period of heightened threat, car parks should be designed in a manner that allows for parts of each car park to be used as pick-up or drop-off points without unduly interfering with traffic flow.

Traffic-management planning should consider the entry and exit points to and from the facility and how this can be managed during periods of heightened threat. For example, a relevant question is, if car park capacity is reduced due to the displacement of the pick-up and drop-off points, can vehicles entering the airport be turned away before they enter the airport's internal road system?

The entire traffic-management infrastructure design should provide for unobstructed access and exit of emergency vehicles to and from terminal frontage and other landside facilities deemed at higher risk, for example hotels and contingency drop-off points.

Use of parking area as drop off – Courtesy of Montevideo Airport

9.6.1 Traffic management and speed

Beyond providing a physical blockade to a hostile vehicle, slowing of general traffic around airports offers the following benefits:

- Improved road safety, with a reduction in frequency and severity of accidents;
- It provides security resources with time to assess approaching vehicles and their occupants;
- Physical infrastructure for stopping hostile vehicles can be reduced due to lower speeds;
- Vehicle approaches can be blocked and vehicle-impact speeds consequently reduced; and
- The appeal of using a hostile vehicle as a weapon is reduced.

9.6.2 Movement control

Movement control has to involve both pedestrian and vehicular movement. Depending on the type of facility, and location, it may be difficult to achieve ideal control. However, the principles are still applicable:

- **Separating incoming and outgoing traffic**—This allows for more space at the main entry point to screen vehicles properly and also screen pedestrians, if applicable.
- **No direct vehicle lane towards building entrances**—This ensures that vehicles can't accelerate directly towards building entrances, limiting the impact from a deliberate or accidental crash into the building. Heavy bushes, bollards, street furniture and fences can be used to guide the traffic flow.
- **Screening delivery personnel/contractors**—Deliveries and contractors should have a separate entrance into the building and such personnel should be screened upon arrival. Security manpower and screening equipment are necessary at this location.
- **Secured areas**—Certain areas may be off-limits to non-authorised personnel or the general public. Such areas need to be secured properly and marked properly. Authorised access can be achieved using an Electronic Access Control System (EACS).
- **Loading/unloading bay**—It is always good to separate the loading/unloading bay from general public areas, as deliveries often use heavier vehicles such as trucks and vans and such a separation will also limit the possibility of accidents. It also allows for security personnel to observe or even screen vehicles before they enter the loading/unloading bay.
- **Emergency exits/staircases**—It is generally recommended to secure all emergency exits and/or staircases leading out of a building. This limits possible entry points that perpetrators could use to facilitate entry into the building, and it also reduces unnecessary patrol time. Such exits should be secured, but have to be able to open during fire or other evacuation scenarios.
- **Incident response agencies**—These agencies should be consulted so that specific response requirements are taken into account, e.g., control of elevators and escalators during an incident.

9.6.3 Vehicular access

- The road layout should be determined using the unique features of the site and the operational needs of the airport or facility. Airports should have a one-way system towards the terminal building and may employ several lanes, which should be managed and controlled. The layout should, where possible, design out the close proximity of vehicle routes to crowded places. Service vehicles such as delivery trucks and fuelling tankers requiring access to airport infrastructure should be kept away from the terminal forecourt and high-density public areas. Planners need to understand the potential impact probabilities and the requirement to have road access that allows speed to be managed. However, potential terrorists will not necessarily follow traffic laws or use normal vehicle routes.
- As a minimum, the front of the terminal and the perimeter boundary line between the airside and landside should be considered potential targets. The airport's local risk assessment should identify any specific vulnerable points from the perspectives of vehicle speed and direction of approach and impact probabilities should be managed by adopting traffic-calming measures, such as using horizontal deflections (e.g. bends, chicanes, turning junctions and roundabouts).
- The airport should also design out the threat of vehicles laden with explosives (VBIED) impacting buildings where the public congregates in large numbers, e.g., terminal entrances or an airport

hotel attached to a terminal. This can be managed with roads designed to be lower than the terminal, hostile-vehicle mitigation measures and road systems that should be kept at least 30m away from the terminal entrances.
- All vehicle routes should be covered by regular security patrols. The patrol's aim is to ensure that all routes are clear of vehicles and/or suspicious objects. In conjunction with such mitigation, all maintenance staff employed to work in such areas should be briefed on security awareness and be prepared to action an appropriate response.

9.6.4 Hostile Vehicle Mitigation

Where potential penetrative or dynamic attack is identified as a threat, impact-rated vehicle security barriers may be employed. These may be deployed to protect areas of mass gathering or critical structural elements, or in extreme circumstances they can be used to create a closed loop of impact-rated barriers that are capable of stopping hostile vehicles. Five main methods of vehicle-borne attack can be used with or without the involvement of suicide bombers:

- Parked VBIED—e.g., a parked vehicle detonated close to a building asset;
- Encroachment—e.g., exploiting gaps in defences, or tailgating a legitimate vehicle through an active barrier system;
- Penetrative—e.g., a ram attack using a vehicle;
- Deception—e.g.. use of pretence or use of a "Trojan" vehicle; and
- Duress—e.g., against a guard to make the guard open a barrier, or against a legitimate driver to make the driver take an explosive device into his or her own site.

Additional methods of vehicle-borne attack include:

- Layered attacks—i.e., employment of multiple attack methods;
- Surreptitious or forced attack—e.g., tampering or causing damage to a vehicle security barrier or its control system; and
- Explosive charges—e.g., for employment in damaging or removing a vehicle security barrier.

Security thinking regarding HVM defence normally focuses on penetrative attacks. However, it should be noted that a parked vehicle or encroachment attack may also be used at airport terminals. This can be mitigated through the use of non-impact-rated measures.

9.6.5 Secondary Route Contingency Planning

If the main road system is forced to close, planners should also determine secondary routes. A closure may be due to a common vehicular incident, protester action or a terrorist incident. When deciding the road layout, consideration should be given to contingency measures that can be introduced in the event of an incident or heightened threat, for example, the ability to:

- Reverse or change the flow of traffic;
- Ensure vehicles are kept further away from the terminal building by use of traffic controls such as lights or barriers, which may be installed either permanently or temporarily at key locations; and
- Introduce random roadside vehicle checkpoints.

When planning vehicle routes, consideration can be given to seeking advice from local law-enforcement agencies and fire and rescue services.

9.6.6 Service Deliveries

As best practice, delivery vehicles should be kept away from terminal buildings and made to use a separate route. This particularly applies to large delivery vans and large high-gross weight vehicles, particularly fuel carriers. The route should be controlled in order to prevent unauthorized or suspicious vehicles from entering the delivery areas. Airports should have a suitably located access point for airside deliveries.

For larger operations, it is ideal to have a larger facility act as a single point of delivery landside, located at a suitable distance away from terminal buildings and areas of larger crowds. This should be planned accordingly. Using such a facility, deliveries can be separated, identified, screened and shuttled into airside areas in dedicated vehicles (as 'known' secure goods).

9.6.7 Vehicle lanes and drop-off zones

It is common practice for vehicle lanes and drop-off zones for buses, taxis and other vehicles to be placed as near to airport terminal entrances as possible for the convenience of passengers. However, it is recommended that the closest a vehicle lane or drop-off zone should be is a minimum of 30 metres from any terminal entrance. The 30m vehicle exclusion zone should be protected by a vehicle security barrier, because this reduces the likelihood of a VBIED attack potentially causing mass casualties and infrastructure damage, and providing publicity for the perpetrators.

For existing buildings where a 30m vehicle exclusion zone is not possible because of site-specific factors, a formal risk assessment should be carried out and mitigating measures put in place. One measure that may be considered is the siting of an 'authorized vehicle lane' where access is restricted to known vehicles driven by known drivers. Driver authentication should be achieved by having a security presence or using a personal token or personal PIN. Authentication for vehicles must take place prior to entering the lane and vehicle authentication should be through a system that can automatically recognize number plates. Number-plate recognition systems will be discussed later in the handbook. This approach reduces the likelihood and impact of an attack by reducing the means by which perpetrators may get close to the target, the terminal. However, it does not fully mitigate all of the risks and therefore in cases where an authorized vehicle lane is within the 30m zone there should be a vehicle security barrier to prevent hostile vehicles penetrating the

Drop off zone – Courtesy of Atlanta Airport

terminal building. This vehicle security barrier should be located in the area between the authorized vehicle lane pick-up/drop-off points and the terminal.

Some airports have alternate drop-off lanes in regular car parks, allowing for a 'free' 15–20 minute stop. Vehicles lanes and drop-off zones should be regularly monitored to prevent drivers parking and leaving vehicles unattended. Planners should also consider blast-fragmentation of structures within the area.

Airport planners should consider how the airport infrastructure might cope with additional measures that may have to be applied at times of heightened threat, for example where the threat level rises to critical. These could include, for example:

- Closing any Authorised Vehicle Lane with less than a 30-metre stand-off distance from the terminal building or other critical infrastructure, e.g. the air traffic control tower; and
- Moving public vehicles even further afield from outside of the 30-metre zone to a suitable alternative location.

9.6.8 Parking garages

At many airports, the parking garages are essential for travellers and greeters and are strong revenue providers for airport operators. However, they can be targets for unlawful activity. The location of parking garages is determined by the site footprint and the operational needs of the airport. However, parking garages should not be designed or located so as to compromise security. Parking garages should be located to ensure that vehicles are kept at least 30 metres away from terminal buildings and high-density public areas. If parking garages are located adjacent to an airside area boundary, a 3-metre clear zone should be maintained. If this is not possible, the perimeter security must be enhanced to ensure that vehicles parked against it do not compromise aviation security.

When designing multi-storey parking garages, airport planners should seek to prevent them (and any raised ramps leading to them) from potentially allowing direct threats against restricted areas. Additionally, it should not be possible to place prohibited articles in such areas.

Consideration should be given to the risks of a VBIED within a multi-storey car park or detonation of a PBIED. The explosive forces within the confines of a multi-storey cark park are higher than in an unenclosed environment, so the structure of the car park should be capable of withstanding collapse. External cladding should be robustly fixed in order to prevent it from being detached from the façade of the car park and becoming a lethal element. Solid panels and glazing should be designed to remain attached to the car park structure in the event of an explosion or be designed to vent, allowing the explosive expanding gases to be released.

Staff parking garages are generally designed with access control to deny public use and staff members that are authorised to use them are security-cleared. Verification checks and the list of authorized persons should be reviewed regularly. It is advised that staff-parking garages are placed adjacent to airside areas instead of public access car parks as this could reduce the risk to such areas, although the insider threat should always be considered. The opportunity to drive a vehicle through the fence line at speed should be risk-assessed and use of security barriers specially designed to stop vehicles can be considered, particularly where a breach of the fence line would result in entry to the restricted area.

9.6.9 Rail and bus stations

Today, airports are increasingly developing multimodal transit hubs for the cities they serve. In doing so, large transit facilities for bus or trains are being constructed to provide customers with attractive choices for transport to and from the airport other than personal vehicles.

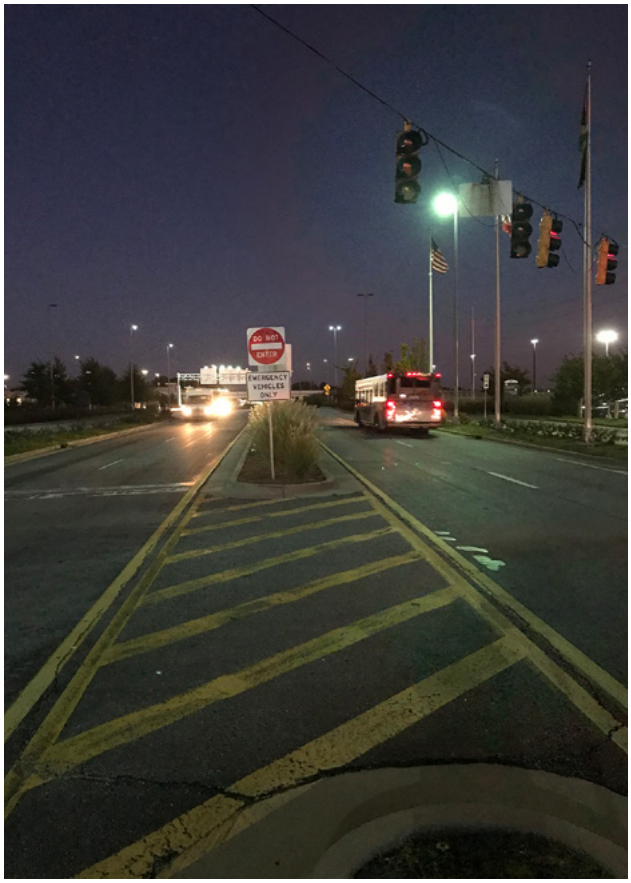
Given the attractiveness of bus and rail stations as potential targets for terrorism, it is highly recommended that physical security measures are in place in stations at airports. The routes between bus and rail stations located within the airport campus should be designed where possible to minimize the need for large groups of people to congregate and to help the free-flowing, controlled movement of people. Pedestrian routes should be adequately lit and covered by CCTV. Where parts of the route may be used to facilitate security contingency arrangements, the requirements should

be taken into account at the design stage, including the need for communication systems for emergency announcements. Such routes may also serve as escape routes from the terminal in an emergency and should be designed with this in mind.

9.6.10 Emergency vehicle access

The airport operator should have provisions in place to allow for easy access for emergency vehicles. While the airport security force aims to protect the travelling public and airport community from threats, there is also a need to consider how effectively the security department works together with airport safety to mitigate any potential conflicts that may arise. Examples of effective security and safety cooperation include:

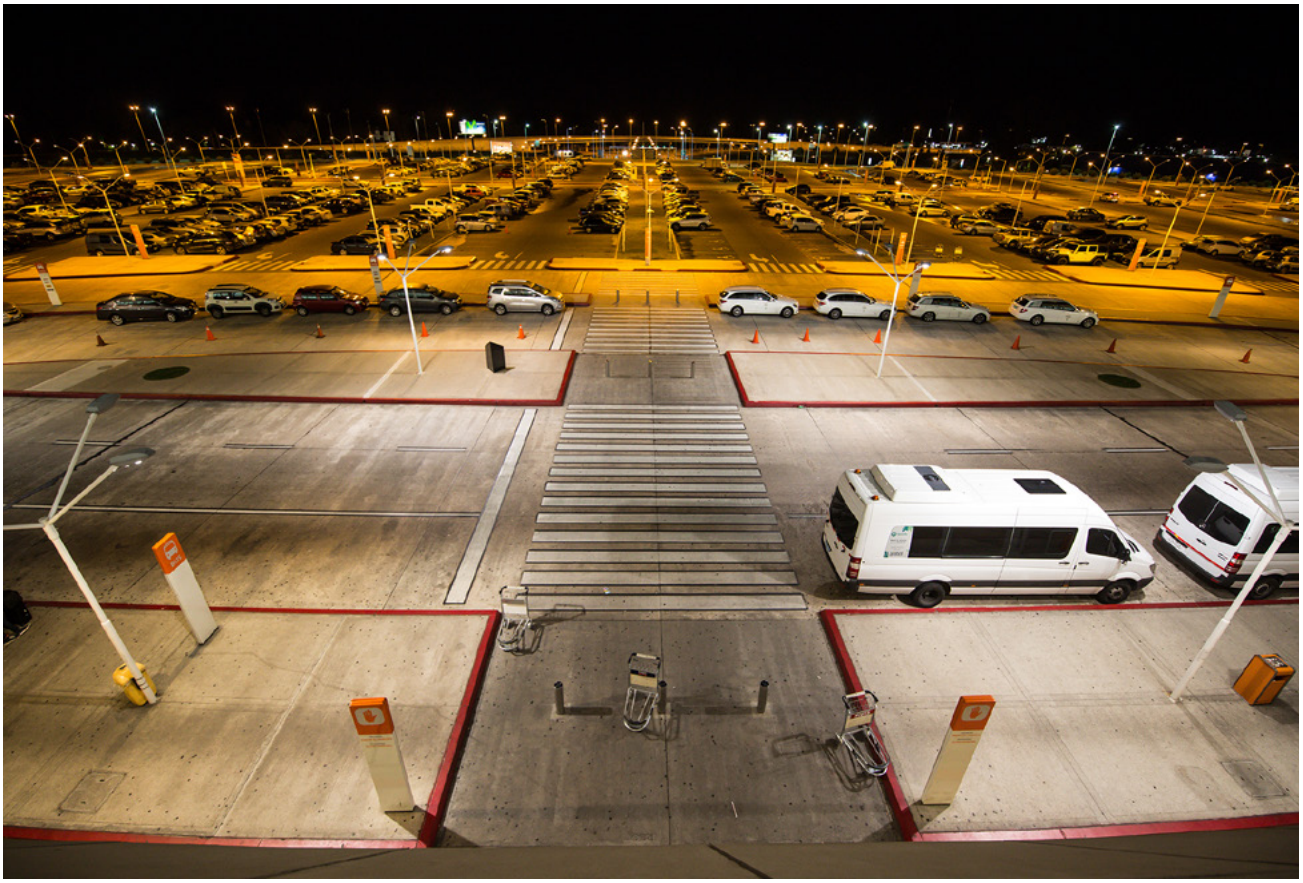
- Communication of information to relevant parties to manage the incident effectively and not draw unwanted attention to a vulnerability that may be exploited;
- The ability to restrict access to the incident site only to emergency services (with coordination through the security/safety officer), to minimize exposure to hazards;
- Designating a marshalling point that does not expose the public to other hazards and a contingency location if that marshalling point is rendered unfeasible;
- Providing traffic-management measures such as cordons and road closures to prevent road and pedestrian traffic exposure to further hazards; and
- Provision of emergency access through crash/sliding gates or laneways of appropriate width (where applicable) for incident management, while also delivering access control at a suitable level for a given area, including access for Aviation Rescue and Fire Fighting Services. Please keep in mind that fire vehicles need sufficient manoeuvring room to be able to take up effective positions from which fire-fighting or emergency operations can take place. These vehicles are usually around 10m long, 3.5m wide and 4m high and weigh approximately 30 tonnes. Another issue to consider is where bollards are used and emergency services cannot get access, either because keys are unavailable or because bollards do not operate and have become unserviceable due to lack of use or maintenance. Planning or consideration will be necessary for emergency responses as any delay in response results in a longer intervention time.



Emergency vehicle access – Courtesy of Atlanta Airport

9.6.11 Pedestrian access

To protect the external area of the terminal building, adequate methods of facilitation must be in place to allow pedestrians to move in the most efficient manner possible, both during normal operation and during the response to an attack. Terminal external pedestrian areas are areas immediately in front of the terminal structure and are used by pedestrians only. The aim should be to allow people entering the terminal buildings or exiting the terminal towards parking garages, bus stops and train stations to move quickly and easily through an area that has minimal hazards. This limits large numbers of people congregating and reduces the chances of crowds potentially forming attractive targets. Hostile vehicles should not be able to compromise the measures provided to facilitate pedestrian access.



Pedestrian walkway – Courtesy of Montevideo Airport

To deter the attraction of using commercial vehicles as a threat, commercial operations should not be conducted in front of terminal buildings. If seating is provided outside the terminal—for example, adjacent to help points for disabled persons and their caregivers, for smoking shelters and for persons awaiting public transportation—the seats should be designed to take into account the risks associated with waiting in this area. If possible, such seats should be limited in number, sited as far away as possible from uncontrolled vehicles, constructed of materials that will not fragment under blast loading and be shielded where possible with such items as planters or purpose-made shelters designed to be blast-resistant. The design of the foundations of any shelters is critical to the ability of the shelters to withstand blast.

For terminal-entrance areas leading into the departures area of a terminal, people should be able to move as quickly as possible into the terminal behind a protected structure. The design should ensure that there is no unnecessary infrastructure within the pedestrian forecourt area that could cause an additional hazard to people. Departures areas should, where possible, generally be clear of visual obstructions such as fixed litter bins, bus-stop shelters and large advertising hoardings, to facilitate a clear overview and allow surveillance to limit the scope for concealment of an improvised explosive device. Security should be built into landscaping—for example, trees should not impede sightlines of existing or proposed CCTV.

Arrivals areas prove more challenging, because these areas may require people to congregate while they

queue for taxis or public transport. Consideration should be given as to whether infrastructure can be designed to provide defences against blast fragmentation and firearms. The design of the external pedestrian area should take account of contingency-planning arrangements and should be discussed with the security management team. Areas outside the terminal that may be used for holding people prior to entry, or to undertake additional checks on persons entering the terminal, require extra consideration. It is recommended that these areas have adequate power, lighting, heating, shelter, space for equipment, and data and communication, and that passenger welfare requirements are in place in case of contingency.

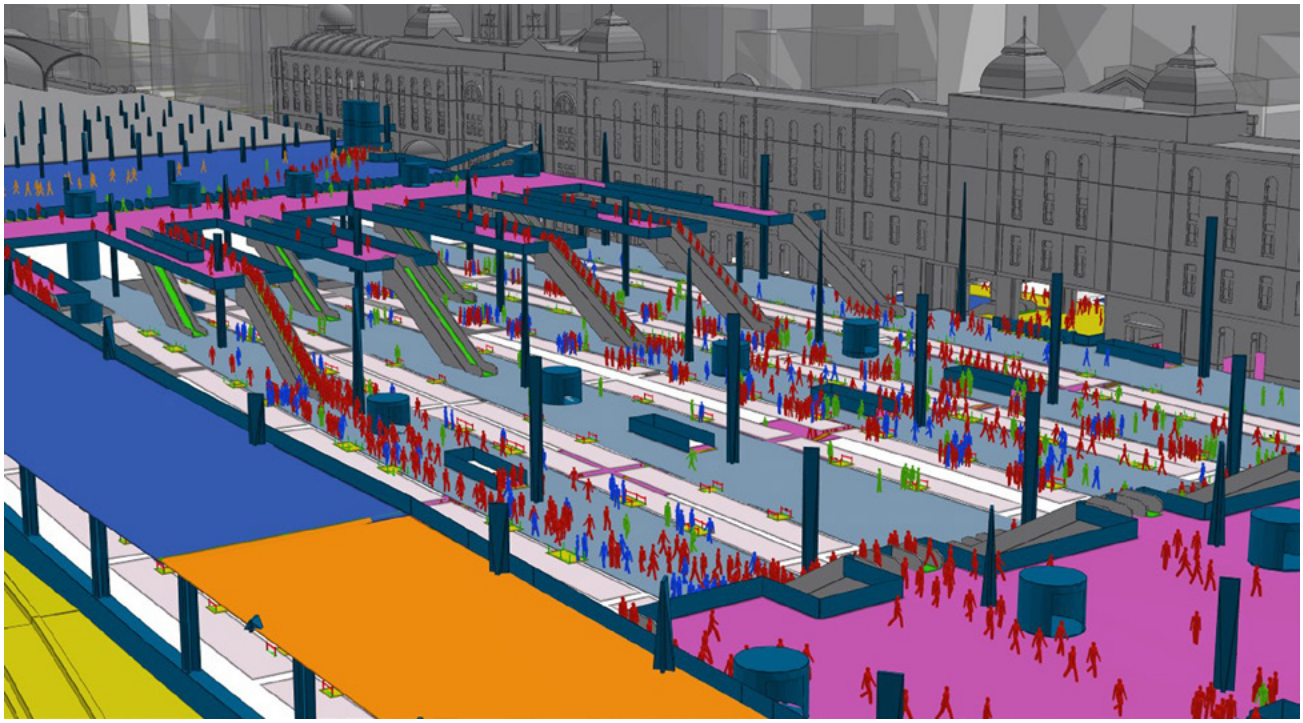
Canopies can provide cover at terminal entrances and exits. It is recommended that they are constructed in a manner in which the structural components will remain in place in the event of an explosion, but that the interconnecting roofing panels, fabric, etc. are able to vent the explosion in some way—for example, by peeling upwards or backwards.

9.6.12 Landside wayfinding, acoustic engineering and signage

Wayfinding for vehicles should be designed to facilitate efficient movement of traffic through the areas of greatest vulnerability and should be aligned to the hostile-vehicle mitigation measures use to manage speed of vehicles. The risk assessment will indicate the areas of vulnerability and the use of pedestrian-planning applications will assist in mitigating these as far as is reasonably practical.

9.7 Vulnerable operation points

A business-impact analysis will identify those functions that are critical to business continuity. The risk assessment should identify the risks that could impact on these critical functions. Where possible, these functions should be located in security-restricted areas which, by the nature of their location, will reduce the residual risk.



Example of a typical pedestrian planning model

Examples of vulnerable operation points include utility plants, emergency response facilities, data centres and air navigation facilities.

9.7.1 Line of sight

Providing line-of-sight capability in the conduct of overt and covert surveillance increases the deterrence value of patrolling and likelihood of detection. However, this design feature may conflict with measures that can be utilised to mitigate against an armed assault. These measures demand interior structures in which people can hide in the event of an attack.

Line of sight for the purposes of surveillance equally provides attackers with a line of sight. The risk assessment should consider this vulnerability. Particular attention should be given to publicly accessible facilities that overlook attractive targets—e.g., viewing terraces which overlook check-in areas. Security measures may be required to address vulnerabilities in existing infrastructure. Once measures have been put in place, operators may be able to exploit these spaces to deter, identify and respond to any threats.

9.7.2 Concealment

The number of locations in which packaged threats—e.g., IEDs— can be placed should be minimized. This can be achieved through the building's architecture and interior design designing out features that may facilitate concealment and by selecting fixtures and fittings such as open-base chairs, clear garbage bins and public-realm design.

Neighbouring campuses airports, in particular, are increasingly looking for opportunities to increase revenue through non-core business. This often manifests as constructions located landside, some of which service the airport and users (such as car parks and hotels) and others which are only co-located, e.g. business parks. These facilities will influence the risks to the airport in one of two ways: the neighbouring facility may be liable to security risks in its own right and its construction may increase the risk to the airport's landside. An example of the former risk is a crowded hotel check-in area. An example of the latter risk is a VBIED being parked in a neighbouring facility's car park but able to target airport users.

9.7.3 High-risk operations

Airports may host the operations of high-risk carriers. Consideration should be given to the location of the operator's required terminal operations, including its check-in facilities and offices. The relevant elements of the risk assessment should be performed in consultation with the operator, noting that the operator may have security specifications which need to be accommodated in the design. In determining the location of the terminal operations and security specifications, consideration should be given to facilitation and efficiency of common-use terminal equipment, including the resilience of fixtures and fittings.

The scope of the risk assessment should consider these facilities and balance the likelihood, consequences and mitigation measures of such developments.

9.8 Non-public areas

9.8.1 Service corridors, stairwells, and vertical circulation

Service corridors may be desirable to enhance public aesthetics by concealing service and delivery activities, and they can increase airport efficiency by providing clear, unobstructed pathways where airport personnel can quickly traverse the terminal.

Service corridors may transit a portion of or the entire length of the terminal. To avoid unauthorized access to secured or sterile areas, service corridors should not cross area boundaries. If crossings cannot be avoided, transitions should be minimized, access-controlled, and consider surveillance requirements.

Service corridors may also be used to minimize security access points. If access requirements are grouped together with similar personnel or tenant areas (such as airline ticket offices, concession storage areas, concessionaires, and equipment-maintenance access points), a common service corridor may serve multiple entities, and may provide greater control of security than separate access points for each user.

The planning and design of service corridors should consider their placement and possible use by airport

emergency personnel and law enforcement agencies. While use of service corridors by emergency and law enforcement personnel is not a security requirement, proper corridor placement and design characteristics can enhance response times as well as allow for private, non-disruptive transport of injured persons or security detainees.

Vertical-circulation facilities such as escalators, elevators, and stairwells are more difficult to control than corridors. They provide access not only to multiple floors, but often to multiple security levels as well. In particular, fire stairs typically connect as many of the building's floors or levels as possible. Since they are located primarily to meet code-separation requirements and provide egress from the facility, they are not often conveniently located with regard to security boundaries or the airport's operation. Thus, additional non-fire stairs, escalators, and elevators are often needed as well. Optimally, vertical cores are shared for egress and operational movement.

9.8.2 Airport and tenant administrative/ personnel offices

Airport, airline and tenant personnel require support space throughout the terminal facility for various functions. Types of airport personnel offices typically located within an airport terminal include airport administrative offices, maintenance support offices, law enforcement facilities, ID offices, and security department offices and substations, as well as airline and tenant (including government agency) offices.

Administrative offices are best located close to the main bulk of the occupants, to minimize the need for multiple security transitions. There may be various office areas within multiple security areas depending upon the functions and preferences of the airport personnel. Ideally, office areas should be located and connected via corridors and vertical circulation, to minimize the amount of office staffers who need to cross security boundaries in their daily activities. Likewise, office spaces should be planned with consideration for visitors and public access, as well as the likelihood that those visitors might be inadvertently left unattended or unescorted, providing unintended access to security areas.

Consideration should be given where appropriate to the use of remote police facilities and first aid offices that allow for easy public access and the possibility of more efficient response times.

When airport operator/administration offices are located within a public terminal, these areas should be equipped with security access-control equipment and/ or monitored by CCTV or patrols. It is typically more cost-effective and efficient to use a single security system for all requirements. These areas usually require security door treatments, duress alarms, and connection to the airport operations centre and monitoring equipment.

9.8.3 Tenant spaces

In terms of tenant space access, there is no fixed rule on whether tenant spaces require tie-in to an airport security access-control system. Some states do not require tenants to have a security program, but if the airport wishes to include tenant areas, it is wise to design a single system rather than try to integrate multiple tenant systems. Collaboration with tenants, and perhaps with a representative of the tenant community as a whole, should be performed to ensure such protection requirements as those for money-handling operations, high-value cargo, overnight cargo and maintenance operations, and late night or early morning concession deliveries.

10 FACILITATION OF PASSENGER FLOWS

The security risk to terminals largely exists because a target-rich environment is created by the gathering of people in an unfamiliar environment. Protecting the target—or the gathering of people—can be achieved both by overtly protecting the crowd and reducing the crowd's size and therefore its attractiveness as a target.

Achieving crowd minimization provides mutual benefits to security and passenger-experience objectives. It is likely that the latter consideration will be the driving force in an operation with a focus on passenger experience. Crowd minimization can be facilitated through a combination of environmental design and passenger-focused operational processes.

At a macro level, environmental design is driven by capacity needs. Ports and airport security should be consulting with their respective capacity and design planning businesses so that crowd minimization and security measures that have a space demand are taken into account. Understanding capacity impacts, coupled with security requirements, can inform asset reconfiguration or refurbishment of existing operations. The latter process should take account of the location of crowds inside the terminal relative to less secure areas outside or in other parts of the terminal. For example, terminal design, asset reconfiguration and asset refurbishment may be accompanied by operational process changes to facilitate crowd minimization.

Operational processes typically create a choke point in the passenger's journey through the terminal and this creates crowding. Addressing these checkpoints through process improvement or elimination can result in eliminating crowds altogether, or reduce the number of people in a crowd and/or disperse the crowd. Operational process changes may be the responsibility of organizations other than the airport. Additionally, process changes may result in displacement of crowds. These issues demand coordination and cooperation of all involved, including asset owners, airline operators and relevant government authorities within the setting being examined.

The following are examples of operational processes that can assist with crowd minimization:

- Traffic control: implementing an effective traffic-control process;
- Maximum utilization of check-in counters by airlines: this improves the throughput of passengers through the check-in process, reducing crowds;
- Using check-in kiosks: assuming sufficient capacity, this spreads the crowd compared with queues that form for slower manual check-in and bag-drop processes;
- Removing check-in: increasingly airlines are expecting their passengers to check in online. Taking this process out of the terminal removes one choke point completely;
- Use of bag-drop facilities: assuming sufficient capacity, as with check-in kiosks, this spreads the crowd more than queues formed for the typically slower process of manual check-in and bag-drop;
- Wider implementation of baggage and check-in processes/mechanisms that speed up the check-in and bag-drop processes; online check-in is a widely adopted mechanism for the former. Consider using permanent electronic bag tags or e-tags—home-printed bag tags are an example of the latter;
- Wider use of bag-delivery services: these services facilitate the transfer of baggage from point to point and avoid the need for passengers to check in or drop bags in the terminal. Examples in operation include Follow Your Bag, Swiss International Air Lines' door-to-door luggage and check-in service;
- Using off-site check-in facilities—care should be taken not to displace the risk to the off-site location;
- Increasing the throughput at border control via the use of Automated Border Control (ABC) kiosks and passenger screening to minimise queuing;
- Introducing risk-based screening in order to process certain passengers faster, reducing the volume of people in the area before screening; and
- Discouraging loitering of passengers and meeters-and-greeters and minimising retail facilities in the public area.

FACILITATION OF PASSENGER FLOWS

10.1 Design

Good terminal design includes the following features to minimise the congregation of crowds and queues:

- To reduce crowds, departing, arriving and transferring passengers should, wherever possible, stay on one level—for example, departures use one level of a terminal while arrivals use another;
- As far as possible, check-in halls should be light and spacious, providing options for passengers wishing to use automated services as well as catering for those who need assistance, away from the main flow of passenger traffic; and
- Typical areas of mass gathering such as check-in counters, kiosks, entrances and exits should be separated to the maximum distance possible to reduce crowd density and provide a clearer line of sight for surveillance efforts. Self-serve kiosks can be positioned close to the entrance of the terminal building but should be designed to minimize queueing and not create additional crowds.

Wayfinding and passenger orientation can be enhanced by reducing the number of choices to an absolute minimum—e.g., creating one terminal complex by adopting a transparent building philosophy; providing a clear line of sight through the building and providing direct passenger-flow routes; and designing the flow process so no backtracking or changes in direction greater than 90 degrees are involved. All decision points should be binary to make the wayfinding as intuitive as possible and reduce confusion for the customer.

Innovative check-in design – courtesy of Atlanta Airport

Many terminal buildings present challenges by incorporating elevators, escalators, and stairwells that service multiple levels on the public side. One of these methods should be used for access between the boundaries of sterile or secured areas, particularly those leading to and from airport administration offices, boarding gates and passenger hold-rooms, as well as at baggage-claim areas where carousels and doors may provide a direct path between public and secured areas.

From a security-design perspective, it is important to move people quickly and efficiently from one public location to another and to keep them from moving into any area designated as a secured or sterile area. Design solutions such as physically separating people along non-intersecting paths of travel may require methods of access control or directional channeling. When providing passenger-flow solutions for emergency operations, ensure that people are channeled away from secured areas during any evacuation procedures.

10.2 Automated processes

Operational processes typically create choke points in the passenger's journey through the terminal, which in turn creates crowding. Addressing these checkpoints through process improvement or elimination can result in eliminating crowds altogether, or reduce the volume of people in a crowd and/or disperse the crowd. Operational process changes may be the responsibility of organisations other than the airport authority. Additionally, process changes may result in displacement of crowds. These issues demand coordination and cooperation of all involved, including asset owners, airline operators and relevant government authorities.

Through many programs, among them IATA's FAST Travel initiative, work is underway on providing self-service solutions throughout the passenger journey, including check-in, bag-drop, self-tagging, re-booking and boarding processes. According to the FAST Travel vision, "By 2020, 80% of global passengers will be offered with a complete relevant Self-Service suite throughout their journey to provide better convenience and reduce queues."

Emphasis should be placed either on automating and eliminating processes or moving them away from the airport. As identified previously, examples might include remote/mobile check-in and home-printed or permanent bag tags rather than on-site, self-service options.

Future initiatives such as automated identity management using biometrics will provide opportunities to speed up further the passenger-flow process from door to airside. As tools for identity management and biometrics evolve, solutions should be sought that reduce the number of on-site processes such as enrolment and authentication. One such solution is to enable frequent flyers to store their biometric and biographic data on their frequent-flyer profiles.

10.2.1 Check-in

As online and mobile solutions are increasingly introduced to the passenger process, check-in is gradually becoming a thing of the past for many airports and airlines. However, in many airports long queues are still observed at "special assistance" desks, as well as at check-in kiosks. This is particularly the case for charter operators, or operators serving multiple destinations where passengers are less-experienced travellers. Solutions for better passenger flow and reduced transaction time, along with increasing the prevalence of self-service options, can be considered.

To a large degree, queues are influenced by the distribution of passenger arrivals at the terminal, transaction time and peak departure times in terms of slots. Airports can consider providing common-use self-service equipment and allocating check-in desks appropriately to manage peak flows best, avoiding the use of clusters of desks in close proximity for flights departing at similar times. If 24hr kiosk services are not provided, desks should be opened adequately in advance of flight-departure times to prevent the congregation of passengers waiting for desks to open. This is particularly important when passengers arrive at the airport en masse, for example via buses provided by tour operators.

10.2.2 Bag drop

Bag drop is still a major bottleneck in many airports. Automated solutions such as self-bag-drop and self-tagging are starting to be implemented, but while these solutions are still in their infancy they themselves can cause increased wait times. A sufficient number of bag-drop stations, whether manual or automated, should be provided.

Bag-drop desks should only process bags; other transactions requiring more time (such as schedule changes and special requests) should be directed to other dedicated stations.

Two-step bag-drop processes may be more effective than a single-step solution (i.e., printing tags at a remote location or at home). This reduces transaction time and again alleviates bottlenecks.

For automated solutions, human assistance must be on hand to resolve problems quickly and prevent bottlenecks occurring.

Automatic bag drop – Courtesy of Singapore Airport

Self-service bag drop has many benefits, including an attractive business case; availability of check-in and drop-off 24 hours a day, seven days a week; and also the option to provide drop-off at parking places or other remote airport locations.

Other options to reduce transaction times might include self-tagging, either through permanent electronic bag tags or home-printed bag tags (where regulations allow), or tags self-printed at check-in kiosks.

10.2.3 Document check

Document check has been introduced as an additional step in the passenger process for countries requiring visual verification of documents for passengers checking in remotely. Solutions using identity management and biometrics can be explored to remove this bottleneck.

Additionally, new regulatory requirements such as questioning of passengers are being implemented to address specific security threats. This may introduce new touchpoints in the passenger journey and potentially create bottlenecks. It is strongly recommended that passengers not be segregated by destination (and that their destinations cannot easily be distinguished) when carrying out manual checks, because certain groups may provide specific targets for terrorist attacks.

10.2.4 Payment of duties and taxes

At some destinations, payment of government departure tax is a manual process, completely separate from the check-in or bag-drop process. Although this process is not usually under the control of the airport authority, discussions should be raised at the airport security committee level and with local regulators to highlight vulnerabilities resulting from congestion and regard should be given to alternative ways of collecting duties. This may include online options, mobile-payment solutions, inclusion of charges in ticket costs or simply relocating the payment desks to a more desirable location.

10.2.5 Outbound immigration

Some States require an outbound immigration check in advance of security screening. This is another touchpoint that can be automated through better use of passenger data and automatic verification rather than manual inspection of documents. There is an imperative globally for countries to collect advance passenger information; this provides governments with details of biographical data (name, date of birth,

Self-Tagging Kiosks—Courtesy of Adelaide International Airport

gender, passport number and nationality) and can be used to verify the identities of passengers entering and leaving a country. By using technology for reading and verifying passports and boarding passes, or biometrics, the whole identity-verification process can be automated. This requires regulatory buy-in, but can provide efficiencies for the immigration services, a better passenger experience and a security benefit.

10.3 Measurement of passenger flows

The optimum space required and the number of kiosks and desks needed to process passengers efficiently will depend on the terminal environment, passenger behaviours, the airport's IT infrastructure, its regulatory environment and the customer experience the airport wishes to offer.

Generally speaking, measurement of passenger-flow performance indicators will, at a minimum, help to:

- Confirm and improve passenger-service quality;
- Estimate temporary and continuous bottlenecks in the terminal building;
- Estimate future resource allocation at several process points;
- Calibrate automated passenger-flow forecast tools; and
- Provide guidance in terms of floor layout and installation to ease flow and reduce crowds.

Technical solutions to measure the passenger flow within airport terminal buildings and similar facilities have emerged and have been implemented globally over the past few years. Frequently discussed in the airport community, such solutions can deliver various indicators to evaluate passenger-flow performance and thus enable the terminal operator to achieve its passenger-experience improvement goals.

Meanwhile, using various technical solutions, more and more airports have gathered detailed operational experience and have learned more about the advantages and the challenges that these solutions bring. Beside the numerous successful implementations and positive effects on passenger-flow improvement, some airports have actually switched off previously implemented solutions due to the lack of benefits and quality of the results those solutions provide.

The ACI World Airport IT Standing Committee (WAITSC) has developed guidelines on how passenger-flow measurement solutions can be used.[6]

10.4 Passenger preparation and familiarization

10.4.1 Security processes and prohibited items

Security checkpoint processes and prohibited items vary significantly from one airport to another.[7] It is therefore crucial to provide passengers with information on what to expect and what to prepare for prior to arriving at the security checkpoint, to ensure a smooth and seamless experience for the passenger. The most common way of providing information is through airport and airline websites and hotel information systems at hotels located in close proximity to the airport.

In addition to websites, airports are starting to leverage passengers' use of mobile devices. Airports can make use of NFC tags, beacons and QR codes placed around the airport to facilitate downloading of the airport's mobile-phone applications and location-specific data. Dedicated airport applications provide necessary information, such as what can be brought to the checkpoint and LAGs restrictions, if applicable.

10.4.2 Passenger compliance messaging

Passenger compliance messaging can have a large impact on operations, but to do so it needs to be targeted correctly. Analysis of checkpoint data can be useful in understanding what compliance messaging is required. In particular, common causes of unnecessary alarms should be identified and compliance messaging focused on these areas.

More comprehensive analysis of checkpoint data may even lead an airport to introduce different compliance

[6] ACI World Airport IT Standing Committee – Task Force "Best Practice for Passenger Flow Measurement" 1.1 (2015)
[7] Smart Security Guidance Document – Checkpoint Environment

Airport compliance messaging – Courtesy of Atlanta Airport

messaging in different terminals or checkpoints, or change messaging throughout the day. A simple example of this may be the verbal messages that officers provide passengers at the lane; alternatively, where airports have access to dynamic signage, or video projection, messages can even be updated for specific flights.

However, as other lane developments are rolled out, security-officer duties may change and as such there may no longer be a divest officer educating the passenger, but potentially a customer-experience representative speaking to passengers as they enter the checkpoint area.

One airport linked certain flights to an increase in compliance-related alarms at its checkpoint. It identified that language and lack of understanding was most likely the cause of passengers failing to divest correctly, so the airport placed passenger-facilitation officers at the checkpoint to coincide with the arrival of passengers for these flights. The officers were able to speak the passengers' language and communicate the requirements to them. This initiative resulted in a decrease in the number of alarms associated with those passenger groups.

Virtual assistants have also now been deployed in some airports to support passenger education and compliance. It is envisaged that the use of this technology and other technologies such as interactive and language-specific messaging to address language barriers, as well as digital storyboards, will become common in supporting passenger information and education in the context of the security checkpoint.

With ever-changing regulatory requirements and the introduction of new equipment, there will always be significant operational impacts which require the need to educate passengers and staff from the beginning.

10.5 Off-airport processes

Moving processes such as check-in and bag drop offer the ideal scenario for preventing accumulations of crowds and queues. Some airports now offer remote services, such as Hong Kong's in-town check-in process.

In-town check in facilities

Some airlines, resort hotels and tour operators in tourist destinations provide a similar, but perhaps simpler, solution by enabling check-in and bag-drop to take place at hotels the night before departure. Not only do these initiatives alleviate queues at the airport, but they provide good passenger service.

Remote bag check in service – Courtesy of Airportr

A third option is provided by services that offer remote collection and check-in of bags from home or hotels, usually in partnership with airports and airlines.

In any of these scenarios, passengers can proceed directly to the security checkpoint, provided they are not required to perform a document check.

10.6 Departures area

At a macro level, environmental design is driven by capacity needs. Ports and airport security should consult with their respective capacity and design planning businesses so that crowd minimization and security measures that have a space demand are taken into account. Understanding capacity impacts, together with security requirements, can inform asset reconfiguration or refurbishment of existing operations. Refurbishment should take account of the location of crowds inside the terminal relative to those in less secure areas which are outside or in other parts of the terminal.

Terminal design, asset reconfiguration and asset refurbishment may be accompanied by operational process changes to facilitate crowd minimization.

Measures that deliver a good security outcome for the movement of people may also create an environment in which suspicious activities and objects can more readily be detected and resolved.

10.6.1 Management of queues and optimizing utilization

Where queuing needs to be controlled inside the terminal, especially during special events or particularly high traffic peaks, use of retractable, stretch-belt Tensator barriers is appropriate. However, care should be taken in their placement:

- Queues should not be positioned where they may result in the formation of queues outside the building, or adjacent to the building façade or the terminal entrances;
- Queues should not be positioned where they will obstruct the flow of passengers to other services or areas;
- Sight lines should be considered, in order to eliminate possible hiding places;
- Planned emergency-escape routes should not be hindered;

- The ceiling areas above high-density queuing areas should be reviewed in order to minimise injury in the event of an explosion within the area;
- It should be borne in mind that Tensator barriers themselves may cause injury in an explosion, so their use should be controlled;
- If the queue is predictable, fixed barriers may be preferable, in order to a) provide some protection to the people in line; and b) prevent stanchions/posts causing injury; and
- The entrances to queues should be obvious—if passengers are presented with several entrances and unclear signage, this will cause hesitation and bottlenecks.

Deployment of additional personnel may be considered as an active strategy to manage queues where crowds are forming, again in response to an unusual or peak event.

10.6.2 Kiss and fly area

Many airports experience large gatherings of relatives and well-wishers around the entry to the security checkpoint. Best practices for design can be considered, along with information campaigns to discourage large parties. Separate "relative" zones are also provided in some airports.

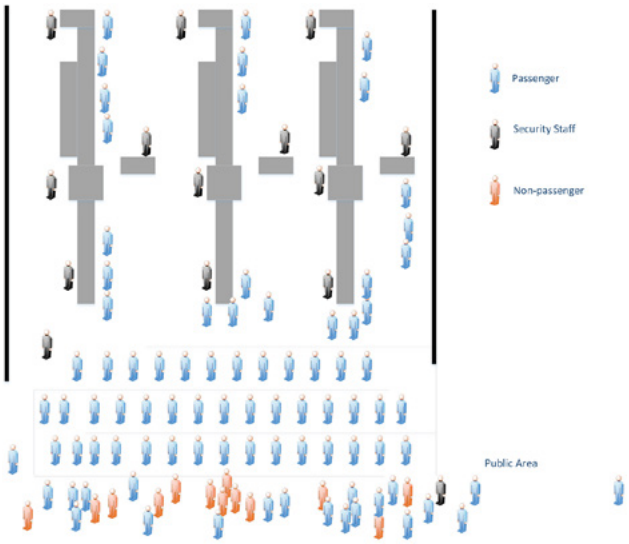
San Francisco International Airport, for example, provides a special zone outside of the terminal building specifically to avoid congestion at terminal curbs.

10.6.3 Security checkpoint queues

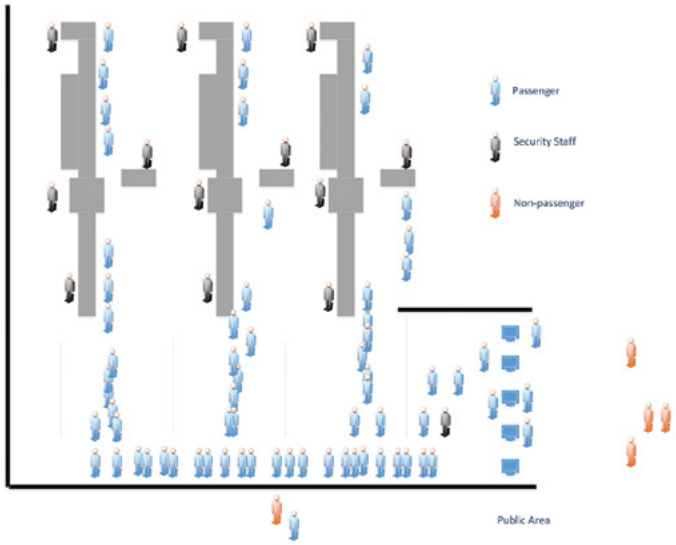
There are many initiatives underway to increase the efficiency of the security checkpoint. However, resourcing and efficiency remain an issue, causing long wait times and large queues. Queue design may be considered in terms of protecting passengers, while also taking into account standardized and robust wait-time metrics and required performance levels for checkpoints.

In a traditional checkpoint model, the queue is accessible to the public, leading to mixing of departing passengers, families, trolleys and baggage outside the queue area. This leaves the queue vulnerable to attack, encourages family and friends to congregate and creates a bottleneck with a single access point.

One option for protecting a queue is to locate e-gates before the entrance to the security checkpoint. This



Traditional queueing model



E-gates remove the queue from public area

E-gate entrance to security screening area

can have several benefits: the queue for the security checkpoint can be moved away from the public area and thus can be protected from attack; a greater number of access points can be provided, reducing bottlenecks; and identity-management processes can be automated.

10.7 Arrivals hall

Arrivals halls are often the poor relatives to departures areas in terms of design. However, the arrivals area may be equally vulnerable to landside attack and there are known instances of threats against groups of arriving passengers from specific flights at international airports.

Similar design elements to those identified for the departures area are also relevant in the arrivals hall, including use of blast-proof materials, provision of good lighting, eliminating areas that can be used to conceal objects or persons, and providing clear lines of sight and clear wayfinding.

However, the arrivals area presents its own challenges because it is a significant gathering place for relatives, taxi drivers, limousine-service providers, porters, tour companies and others. The challenges are made more complex by the presence of baggage and there being no finite process or wait time for most people in the area.

10.7.1 Design

Desks for tour operators should be positioned away from the exit doors from the security-restricted area so that there is a clear line of sight and no mixing of people meeting passengers with queues for hotels, taxis and tour companies.

The provision of multiple, numbered "meeting spots" can help disperse crowds, giving people meeting passengers options for nominating pre-defined meeting areas.

Retail concessions and restaurants can provide facilities that will discourage congregation around the doors from the security-restricted area, but these should be positioned so they do not cause congestion around the main passenger flow.

10.7.2 Baggage hall

For many domestic areas of airports, the baggage hall is in a publicly accessed area. This not only creates crowds but also makes baggage vulnerable to pilferage or interference. Segregation of baggage collection from the public area should be recommended.

10.7.3 Transportation

Design features such as the moving of taxi stands and bus stops away from the terminal, and restriction of entry to the area for those soliciting business, might be considered.

Pre-booking of ancillary services such as taxis and hotels by means of airport or airline applications may offer opportunities to reduce crowds in arrivals halls by enabling passengers to depart swiftly from the arrivals area.

Public transportation options should be clearly identified and easily accessed to enable swift departure of passengers. To prevent congestion, ticket machines for public-transportation services should be positioned near the services' boarding locations rather than at the exit from the restricted area.

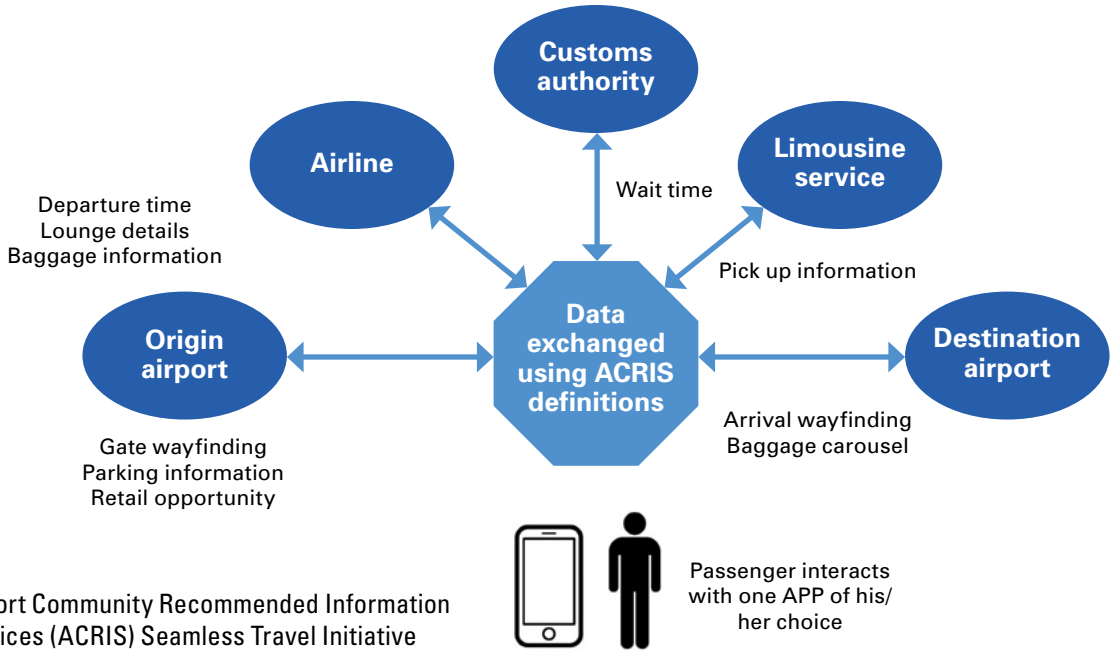
10.8 Technology and the provision of information to passengers

Another area where mobile technology is starting to play a key role is in the provision of timely information for passengers and their relatives.

Applications might include:

- Wayfinding to move passengers quickly to their desired locations;
- Providing security wait times so passengers can arrive at appropriate times before their flights;
- Booking for ancillary services such as ground transportation; and
- Wait times at customs so that those meeting arriving passengers can arrive at the terminal at the appropriate time.

Much of this information is available today through web sites or individual airport applications, but there are now opportunities to bring services together into one application using Application Programming Interfaces (APIs) to exchange functionalities between various stakeholders' apps.



Airport Community Recommended Information Services (ACRIS) Seamless Travel Initiative

Airport wayfinding –Courtesy of Atlanta Airport

10.9 Wayfinding

Wayfinding has a significant effect on passenger flow. Placement of objects—for example, rubbish bins and concessionaire kiosks—or displays of ambiguous information may act as a physical, visual or psychological barrier for self-navigation from one point to another.

Clear signage that provides up-to-date, relevant information can help disperse crowds and prevent bottlenecks.

Some good practices include colour-coding specific paths (such as connections), providing clear pictograms and having dynamic signage that indicates the best path to take. One example of this is Heathrow Airport's indication of queue length at the security checkpoints.

Facilitation may also be assisted by means of supporting communication tools—for example, prompts using public-address systems and passenger-information displays.

11 TRAINING AND SECURITY AWARENESS

All employees working in our airports have an important role to play in ensuring that any behaviours which may be indicative of suspicious or malicious intent are noted, assessed and acted upon. Today, training for security awareness is an ever more critical aspect of ensuring that airports are safe and secure. This chapter will discuss awareness training for all employees in the airport environment, including training for specialist security staff and training for those responsible for emergency response.

11.1 Security staff

Security staff have a number of critical roles in the protection of landside areas. Some of these staff members may be public-safety personnel, security officers or police officers, but often many are directly employed by or contracted to the airport. Training programs for security staff should be appropriate to each job type; specific programs may involve training in access control, patrolling and surveillance, behaviour detection, management of situation escalation, CCTV monitoring and interpretation, crowd management, etc.

Members of the security staff will need:

- Knowledge and skills specific for their jobs;
- Threat awareness, including general knowledge of criminal political groups and terrorist aims and techniques so that they can understand why their role is important and why requirements exist;
- An understanding of the organization of aviation security at the national and local level so that they can understand where their roles fit and where their responsibilities begin and end; and
- Knowledge of airport operations.

Appropriate recruitment and selection also plays a key role in assigning the right person to the right position. Some of the roles above may require a high level of concentration and attention to detail, while others may require greater skills in dealing with difficult people or the ability to act calmly in a crisis.

Following initial training there should also be periodic recurrent training. Training and security awareness may include a mix of training methods such as classroom training, on-the-job training, workshops, role-playing and red-teaming. Interactive learning techniques such as role-playing can be very useful for improving interactions between teams with different responsibilities.

11.2 Airport employees

Whilst a small minority of airport personnel may be 'law-enforcement/police officers' with the power of arrest, the majority are staff members undertaking a wide range of duties, such as parking enforcement, retail sales, airline staff, airport 'here to help' staff, and so on. Providing security training to this employee range can exponentially increase the number of available 'sensors' within the airport environment.

Global recommended practices advise that employees who are issued with airport passes should complete security-awareness training. However, to tap into this valuable additional-'sensor' resource, such training might be expanded to a broader range of employees working landside in the public area. Typical security-awareness programs will include the topics listed below, but particular emphasis might be placed on behavior-detection techniques. Further information is also included in the 'security culture' section of this handbook regarding staff training and motivation.

Training should be operationally focused on security awareness and the ability to recognize unusual or potentially malicious behaviours. Staff members should be able to demonstrate ability and understanding of their public-area security duties. Periodic and continual awareness training should be provided. Using appropriate methods, ongoing testing for competency should be implemented and training records should be maintained.

11.3 Example basic awareness training program

Audience: All staff members issued with airport airside passes. The training may apply to all personnel employed at an airport, depending on national regulation.

Topics might be defined according to the NCASP, and may include:

- A brief history of terrorism;
- Terrorist tactics and current threats to airports and aviation security;
- Overview of the Airport Security Program;
- Overview of regulations;
- Roles, responsibilities and expectations;
- Partners in security;
- Human factors involved in security;
- Requirement to report suspicious items, persons, etc.;
- Monitoring and patrols—resources available;
- Secure areas:
  - Restricted
  - Sterile
  - Isolation areas (passenger, baggage, aircraft);
- Airport pass system;
- Vehicle identification;
- Access controls;
- Employee access;
- Non-passenger screening;
- Passenger and cabin baggage screening;
- Restricted-area escort requirements;
- Physical security:
  - Barriers, signage, systems
  - Key, access cards, door code control;
- Prohibited items—recognition of items; and
- Incident response.

11.4 Example airport landside and public area security-awareness training

Audience: All staff and contractors working in public areas. This training may be expanded to airport taxi drivers, concessionaires and others.

Topics may be in addition to those above or as a separate course for additional personnel:

- Acknowledge that everyone is responsible for keeping passengers and the airport safe;
- Context and historical reasoning for why it is important;
- How to recognize suspicious behaviors and objects;
- How to recognize and report a potential vulnerability;
- Enable and encourage all workers to express concerns; and
- How to report concerns.

11.5 Dealing with threats

11.5.1 Telephone

Call-centre staff, information-counter staff and any other persons likely to answer a telephone number available to the public should be instructed in how to handle threats received by telephone. Consider that the member of staff who receives the threat may not be prepared—receiving such a threat may be the closest that many people ever come to acts of terrorism—so offer some basic advice to staff members on handling a threat.

1. Stay calm and listen.
2. Obtain as much information as possible. Try to get the caller to be precise about the location and timing of the alleged threat and whom he/she represents. If possible, keep the caller talking.
3. Ensure that any recording facility is switched on.
4. If you have caller ID, note the number. If not, when the caller rings off, retrieve and note the caller's number if you have the facility to do so.
5. Report the incident immediately to the relevant manager or security team for them to decide on the best course of action and to notify the police. If you cannot get hold of anyone, inform the police directly—even if you think the call is a hoax. Give your impressions of the caller and an exact account of what was said.
6. If you have not been able to record the call, make notes—as detailed as possible—on the time and content of the call and your impressions of the caller, for the security staff or police.
7. Do not leave your post—unless ordered to evacuate—until the police or security staff arrive.

An example of training that could be given to staff regarding bomb threats. Courtesy CPNI.

11.5.2 Social media

Employees monitoring airport social media or following airport/airline social-media accounts should be alert to potential threats against the airport and understand when and how to report suspicious activity.

11.6 Response team

A subset of employees, including security and non-security staff, may be identified as a response team with specific duties in times of heightened threat or crisis. The subset may include:

- Airport workers who may be tasked with response duties;
- Mutual-aid responders who have specified roles during a crisis or incident; and
- Federal/state agencies, which may have specific oversight roles.

Proper training should be conducted so that if there is a need to search or evacuate the terminal or airport, every airport employee—not just the search teams—will know what to do. Regular search and evacuation drills help maintain staff awareness and vigilance. All staff members should be made aware of the evacuation assembly points.

Other key staff members such as evacuation marshals should know their roles and be trained regularly. It is important that all employees recognize those who have been specially nominated and obey their instructions. Procedures should ensure that nominated staff are replaced when they leave or are temporarily absent, so that there are no lapses in coverage.

11.7 Exercises and drills

Organizing regular drills and exercises will help familiarize staff with procedures and allow details within the plan to be refined. For example, the agreed response to a bomb alert may differ from the agreed response to an active shooter; staff need to understand the differences and why. Drills should include all key stakeholders if possible, including local law-enforcement response teams.

11.8 Staff feedback

Periodically gauging staff opinion about security habits can help determine whether measures and procedures are both appropriate and understood. It is also important to demonstrate that obtaining and using staff feedback is a transparent process by sharing the results of staff feedback—both positive and negative—with all employees, along with any resulting security-enhancing actions taken by airport management and the security staff.

12 BIBLIOGRAPHY

Along with airport and ACI World Business Partner best practices and expertise, the following sources have been used for reference;

Aviation Security in Airport Development – UK Department for Transport, 2016

Landside (Terminal) Security – Best Practice Guidelines (October 2016) – ACI EUROPE

Best Practices for Communication Strategies in Aviation Security (January 2017) – ACI EUROPE

Crisis Communications in the Digital Age – A Guide to "Best Practice" for the Aviation Industry – IATA, December 2016

Smart Security – Checkpoint Design and Automation V2, 2016

ICAO Doc 8973 – Aviation Security Manual, 10th Edition, 2017

Fort Lauderdale-Hollywood International Airport, Active Shooter Incident and Post-Event Response, January 6, 2017 After-Action Report

https://www.cpni.gov.uk/developing-security-culture retrieved September, 2017

ACI World
Suite 1810
800 Rue du Square Victoria
Montreal, Quebec, H4Z 1G8
Canada

www.aci.aero

To access ACI's publications, please visit
aci.aero/publications/new-releases

ISBN 978-1-927907-56-6