The ICAO global Risk Context Statement (RCS) provides a high-level description of the global aviation security risk picture. The statement presents high-level statements to help guide Member States in taking a risk-based approach to maintaining their national civil aviation security programmes.
1. **INTRODUCTION**

1.1 The continuing threat of terrorism is most effectively managed by identifying, understanding and addressing the potential risks both to and from civil aviation in general and its passengers and specific goods (baggage, cargo and mail) transported. Therefore, the ICAO global aviation security Risk Context Statement (RCS) has been developed, and aims to:

- provide a description of the global risk picture;
- assist States in their efforts to protect air transportation and prevent its use for unlawful acts;
- present high-level statements for an improved approach in creating and maintaining State national civil aviation security programmes; and
- assist ICAO in improving Standards and Recommended Practices (SARPs) and guidance material.

1.2 The RCS reinforces the importance of a risk-based approach, provides a risk assessment process map, and explains a methodology developed by the ICAO Aviation Security (AVSEC) Panel Working Group on Threat and Risk (WGTR). The RCS emphasises the importance of States reporting and sharing information if they and ICAO are to apply the risk assessment process effectively. Finally, based on risk assessments already carried out using the suggested methodology, the RCS provides a relative ranking of these risks. A table of the main terrorist risks to aviation is presented in Section 7.

1.3 The WGTR, which regularly provides risk analysis and risk advice to the AVSEC Panel, maintains the RCS and intends to update the statement as needed to reflect recent events and its own updated risk assessments.

1.4 Although most updates to the RCS will first be considered by the AVSEC Panel, the WGTR provides urgent advice directly to the ICAO Secretariat for dissemination to Member States in times of immediate global threat. For example, in response to the attempted attacks through the cargo system in October 2010, the WGTR reviewed its cargo risk assessment and provided suggested mitigation measures to the Secretariat through the WGTR Chairman.

1.5 The RCS is aimed primarily at aviation security decision makers among the Secretariat and in Member States.

1.6 **Role of ICAO in maintaining global aviation security baseline**

1.6.1 When aviation security arose as a serious issue in the late 1960s, the Chicago Convention system of Annexes was adapted to provide an international framework for addressing acts of unlawful interference. In the years since, ICAO has become the world leader in developing aviation security policies and measures at the international level, and the enhancement of aviation security worldwide remains a strategic objective of the Organization.

1.6.2 Provisions for international aviation security were first incorporated into the Chicago Convention in 1974 (Annex 17 — Security), and since then have been improved and updated 12 times. ICAO has also provided States with guidance material to assist with the implementation of the
security measures contained in Annex 17, among which the primary document is the *Aviation Security Manual* (Doc 8973 — Restricted). Aviation security is also addressed in other Annexes.

1.6.3 Standard 3.1.3 of Annex 17 requires each State to keep under constant review the level of threat to civil aviation within its territory, and establish and implement policies and procedures to adjust relevant elements of its national civil aviation security programme, based on a security risk assessment carried out by relevant national authorities.

1.6.4 In addressing the evolving threat to civil aviation, ICAO relies on the advice of experts who sit on the AVSEC Panel. Established in the late 1980s, the Panel currently consists of 27 members nominated by States, as well as five observers from industry. Together with the Secretariat, the Panel actively develops ICAO security policy and responses to emerging threats, as well as strategies aimed at preventing future acts of unlawful interference. ICAO also draws on advice from the WGTR, which provides timely advice on evolving threats and incidents.

1.7 **Importance of threat and risk assessment approach**

1.7.1 The Declaration on Aviation Security adopted by the 37th Session of the ICAO Assembly calls on all Member States to share best practices and information on a range of key aviation security matters, including threat-based risk assessments. The Assembly also directed the Council to instruct the AVSEC Panel to identify and develop a risk assessment methodology for aviation security and to include risk-based assessments with any recommendations for the adoption of new or amended aviation security measures.

1.7.2 A reasonably designed risk-based approach is one by which States identify the criteria to measure potential criminal activities, principally from terrorism. The identification of risks permits States to determine and implement proportionate measures and controls to mitigate against each risk type.

1.7.3 The RCS aims to fulfil the requests of the Assembly and enables ICAO and Member States to put them into effect.

1.8 **Role of States in national and local risk management**

1.8.1 Assessments of national or even local risks, in conjunction with the overall risk factors, provide important and useful information as to potential terrorist methods and types of attack and targets. While the RCS aims to provide a global high-level view of terrorist risks, it does not attempt to create a detailed view of national or local risks, or to suggest that one State has higher levels of risk associated with it than another State. It is therefore the duty of each State to make its own assessment of the risk applying to its territory and assets, and to establish risk mitigation measures, taking into account the high-level view presented in the global RCS.

1.8.2 Each Member State should document and periodically review its risk assessment, or when significant new developments arise, in order to maintain an accurate and up-to-date picture of the risk environment.
2. THE NATURE OF THE THREAT

2.1 For many years, there has been a significant risk to the security of international aviation from terrorists who, for a variety of motives, have sought to carry out acts of unlawful interference against aircraft, or to use aircraft for terrorist purposes. In selecting a target for attack, terrorists are currently likely to consider the following objectives:

- inflicting mass casualties;
- causing economic disruption;
- making a symbolic statement that will generate spectacular media imagery; and
- generating public anxiety.

2.2 All of these are capable of being achieved through attacks on aviation, which explains the particular focus by terrorists on aviation targets, and heightens the need for the effective mitigation of such threats. This combination of issues may lead to a variety of forms of attack on the aviation system.

2.3 Terrorists have shown themselves to be innovative, and may seek out a wider range of methodologies and targets, influenced by the availability and vulnerability of such targets, and the opportunity for success in the terms set out above. The most significant types of possible attack are shown in Table 1 in Section 7.

2.4 Global threat

2.4.1 All national aviation systems are linked to global aviation networks. Decision makers must therefore take into account how the threat to civil aviation is developing globally. This does not mean that threat levels are identical around the world; there are, of course, regional, national and even local variations. However, it does mean that many threats have the potential to very quickly jump national borders and change regions.

2.4.2 The December 2009 ‘underwear bomber’ incident and the October 2010 ‘cargo/printer cartridge’ incident both illustrate how threats can be introduced into the global aviation system halfway around the world and make their way to any State linked to the network. Often, a threat will take the most convenient path through the system; whether that path is convenient because of location, because of its connections to other areas of the system, or because of known weaknesses in that part of the system. Therefore, it is necessary for all States and aviation organizations to pay close attention to threats to aviation, and to be aware of the vulnerabilities and impacts associated with such threats.

2.5 Global consequences

2.5.1 Given the global character of the terrorist threat to the aviation system (and the global nature of the aviation system more generally), it follows that terrorist attacks upon the aviation system have global consequences. Public anxiety and economic disruption caused by a terrorist attack – key terrorist objectives – will manifest themselves well beyond the borders of States that are the locations of terrorist attacks. Even substantially unsuccessful terrorist attacks have the demonstrated ability to achieve terrorist objectives, because the fear and uncertainty that they generate is often no less than that arising from a successful attack. Further, the global span of the media and the internet – specifically exploited by terrorist groups – gives terrorists the ability to reach audiences worldwide via news reporting or their own propaganda, virtually instantaneously.

2.5.2 The 11 September 2001 attacks clearly illustrate the global consequences of terrorist attacks on the aviation system. The attacks themselves were geographically confined to the United States,
but one of the immediate consequences was a historically unprecedented disruption to aviation operations across the globe, arising from the fear that more such attacks would follow elsewhere. The longer-term consequence of the fear and anxiety generated by the attacks was a financial downturn in the aviation industry across the globe. Ultimately, this led to worldwide economic losses measured in trillions of dollars, and the financial collapse of numerous aviation-related businesses.

2.5.3 The global consequences of terrorist attacks on the aviation system mean that an attack upon the aviation interests of even one State is effectively an attack upon the aviation interests of all States. This further reinforces the need for all States and aviation organizations to pay close attention to threats to aviation, even if they do not consider themselves to be directly threatened by terrorist attack.

3. UNDERSTANDING THE THREAT THROUGH INFORMATION SHARING

3.1 According to Standard 5.3.1 of Annex 17, each Member State is obliged to exchange information and report to ICAO all pertinent information concerning the security aspects of an act of unlawful interference. This section is designed to assist States in determining the issues to be reported.

3.2 Types of information

3.2.1 In conducting a risk assessment, it is necessary to assemble information about the threat. Such information may come from a variety of sources, including the following:

- *actual incidents*, including successful or unsuccessful attacks on aviation, which provide information on proven terrorist methodologies;
- *closed sources*, primarily counter-terrorist intelligence, which may be gathered 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.

3.3 Bilateral, multilateral and global information sharing

3.3.1 Lines of communication, both formal and informal, between the aviation security officials of States assist in the rapid exchange of information, including any increase in the threat level. Exchanges of information on techniques used to try to breach security, experience with security equipment, and operational practices, are also extremely advantageous. States are reminded that Section 2.4 of Annex 17 places obligations on them to cooperate in such exchanges of information.

3.3.2 States should develop procedures for the analysis and dissemination of threat information, and to ensure that appropriate actions are taken by aircraft and airport operators to counter an identified threat. Information should be disseminated to individuals on the need-to-know principle, in order for them to effectively carry out their duties.

3.3.3 States with limited resources for dealing with imminent threats should consider negotiating legal and procedural assistance with adjacent States that are better equipped to collect and disseminate threat information.

3.3.4 Details of important developments, such as new or unusual methods of operation and techniques used by perpetrators, should be promptly disseminated to other States and ICAO. While public knowledge of such matters is undesirable, all airports that may experience similar occurrences should be
informed as soon as possible. Such action will facilitate the early development and implementation of effective countermeasures and procedures.

3.3.5 Urgent communications may be facilitated through the use of the ICAO Aviation Security Point of Contact (PoC) Network, established for the communication of imminent threats to civil air transport operations. Pursuant to Assembly Resolution A37-17: Consolidated statement on continuing ICAO policies related to the safeguarding of international civil aviation against acts of unlawful interference, States that have not done so are urged to participate in the ICAO PoC Network.

3.3.6 If a State has specific information about a possible occurrence involving an aircraft operator or airport, it should immediately and concurrently inform the State(s) where the occurrence may take place, directly through the ICAO PoC Network or through the local diplomatic mission. Further, if a State is unable to communicate urgent information to another State, it should immediately request the assistance of a third State or ICAO.

3.3.7 As soon as circumstances indicate that special security precautions may be dispensed with, such information should immediately be transmitted by the appropriate authority to the affected State(s). Finally, as soon as possible after a security incident, a review and analysis of all that transpired should be conducted by the appropriate authority. The results of the review and analysis should be made available to all participants, along with the recommendations of the appropriate authority for general improvement and for the correction of any deficiencies identified. ICAO should be notified, at the earliest opportunity, of any action undertaken by a State to correct a deficiency.

3.3.8 States concerned with an act of unlawful interference should provide ICAO with all pertinent information concerning the security aspects of the occurrence as soon as practicable after the act is resolved. States should, whenever appropriate, furnish copies of reports prepared for ICAO to other States that may have an interest. The categories of incidents that should be reported include:

- unlawful seizure of an aircraft;
- attempted unlawful seizure of an aircraft;
- unlawful act against the safety of civil aviation, including acts of sabotage and malicious damage, and the placing of bombs and other explosive devices or substances in airports, aircraft, baggage, cargo or mail;
- attempted unlawful act against the safety of civil aviation; and
- any other act of unlawful interference, including armed attacks at airports, acts directed toward off-airport personnel, facilities or vehicles, and acts that have the potential to develop into a threat to international civil aviation.

3.3.9 States are asked to consider ways in which they can improve their existing systems of sharing information. For example, some States have established a system of occasional issuance of information bulletins on matters that may be relevant to threats and risks to aviation, which are circulated at an unclassified or official-use-only level through the ICAO Secure Portal. Others have taken the approach of reviewing their own classified information and, if deemed useful to the wider aviation security community, reissuing the information at a lower level of classification to enable its wider dissemination.
4. **TERRORISM AND CRIMINALITY**

4.1 The possibility of a connection between criminality and terrorism should be noted. Criminal activity in the aviation and transportation arenas, when recognized, may point out vulnerabilities in security practices and expose weaknesses in security posture. Where weaknesses are exploited for criminal purposes, they may also be exploited for terrorist purposes.

4.2 Criminals and terrorists use all modes of transportation, including commercial aviation, to travel across nations and internationally across borders, to carry out their missions. Criminal activity may provide funding and/or financing for terrorist groups and activities. As States continue to seize terrorist assets worldwide, extremist groups resort to criminal activities to fund their operations of violence and terror.

4.3 Criminal activity may also be used by terrorists in attempts to test specific security measures and learn how to overcome them. The following criminal activity can sometimes be linked to terrorist activity or the funding of terrorist groups and activity:

- *surveillance* (of security systems, processes or habitual activity in any setting), which may be covert or overt;
- *smuggling* of humans, drugs, cash and/or contraband; and
- *drug trafficking*.

4.4 Identifying criminal activity in the aviation security environment may lead to identifying terrorist activities or evidence of support to terrorist missions. Any unusual or increased incidents of criminal activity in transportation sectors should be noted, and where practicable, shared amongst relevant State agencies and jurisdictions, such as law enforcement, and between States.

5. **INSIDER VULNERABILITIES**

5.1 In development of the RCS, the insider vulnerability has not been considered as a separate category. Instead, threat types have been considered with an insider element included within each category. It is suggested that States adopt a similar approach in developing their own security risk assessments. For instance, in considering a threat category such as a person-borne improvised explosive device (IED) used to attack aircraft, those conducting an assessment should consider, separately, both a passenger-borne IED used to attack aircraft and a person-borne IED introduced by crew and/or employees and used to attack aircraft. It is easy to see how the risk from a particular threat may differ when one considers an insider, such as an aircraft operator staff member or a passenger, as the means of introducing a threat. For example, the:

- *vulnerability* associated with insiders might be considered greater if they have access to the last layer of security in a way that a passenger does not;
- *likelihood* associated with insiders might be less if they have already been subject to vetting and selection procedures and/or screening; and
- *consequence* of a threat associated with insiders might be greater if an insider has access deeper within the system. For instance, an insider could perpetrate a more credible and thus more disruptive hoax.

5.2 In summary, the methodology involves considering each role within the system and whether it offers a particular tactical advantage in relation to each threat type or whether it poses the same issues as passengers. In applying this methodology, it is possible to consider insider vulnerabilities as part of an integrated risk assessment.
RISK ASSESSMENT METHODOLOGY AND PROCESS MAP

Diagram 1. Process map
The purpose of the risk assessment methodology and process map is to assist States in performing a risk assessment of possible and/or potential concerns, and to ensure that careful thought is given to the evaluation of risks. The methodology comprises three primary processes:

- identification of the inherent or theoretical problem;
- residual risk assessment; and
- recommendations.

Risk assessment is a process that evaluates the risks by:

- **Threat Identification** – identifying the threat scenario, consisting of a defined target (e.g. airport terminal or aircraft), as well as the means and method of possible attack (e.g. attack by passenger using an improvised explosive device, or attack by an insider using weapon, etc.);
- **Likelihood** – considering the probability of the threat occurring;
- **Consequence** – assessing the nature and scale of likely impacts associated with a successful attack, including consideration of human, economic, political and reputational factors (based on a reasonable worst-case scenario);
- **Vulnerabilities** – evaluating the effectiveness and vulnerabilities of current security measures (i.e. security strengths and weaknesses of SARPs) in mitigating the potential threat scenario identified; and therefore
- **Residual risk** – assessing the remaining risk of that type of attack being successfully carried out against that target, to enable a judgement to be made as to whether that is acceptable in risk management terms.

It is important that an evaluation using the suggested map carefully identify the possible or potential scenarios, considering each form of threat as thoroughly as possible. Threats might be directed at specific airports, terminals or aviation infrastructure, such as aviation fuel farms, air traffic control facilities or navigational equipment, as well as aircraft, including different forms of aviation, such as general aviation, passenger aircraft, and all-cargo aircraft. The means and methods by which a threat could be carried out should also be evaluated, including how a weapon or explosive device could be constructed or concealed, and the means by which these threat forms might be conveyed, whether person- or vehicle-borne, in order to perpetuate an act of unlawful interference, and who, for example staff, might perpetrate or facilitate such an act.

In the evaluation of the vulnerability of a particular aviation operation and the likelihood of such an attack, the ease with which such an attack could be made, and how attractive the target might be to potential terrorists, should be considered. In general, targets that could generate significant media attention are considered attractive targets and raise the likelihood of such a threat.

Also the higher the consequences, and the more catastrophic the possible impact of an attack, the higher the threat. States could consider using this risk assessment methodology as a model for their own risk assessments. States may wish to consider the vulnerabilities of their own regime and that the risk might not be adequately mitigated by the baseline set forth in Annex 17.

It should be noted that one of the principles used in the assessments has been the consideration of a reasonable worst-case scenario, and resulting risk assessments were evaluated in view of the current SARPs in Annex 17. For risks not sufficiently mitigated, the WGTR proposes amendments and updates to Annex 17 and the *Aviation Security Manual*.

For States wishing to apply this methodology to their risk assessments, the resulting residual risks that are uncovered should be reviewed to evaluate whether they are acceptable or not and, where not, possible additional security measures evaluated to see whether they would be effective, practicable and sustainable.
### 7. THREAT ANALYSIS

<table>
<thead>
<tr>
<th>THREAT TYPE</th>
<th>LIKELIHOOD</th>
<th>CONSEQUENCE</th>
<th>VULNERABILITIES</th>
<th>RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIRBORNE THREATS (conventional hijack)</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>LOW</td>
</tr>
<tr>
<td>AIRBORNE THREATS (aircraft used as weapon)</td>
<td>Medium-Low</td>
<td>High</td>
<td>Medium-Low</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>PERSON-BORNE CONVENTIONAL IMPROVISED EXPLOSIVE DEVICE (IED) (traditional IED with metallic components)</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>PERSON-BORNE NON-CONVENTIONAL IED (low or no metal content and/or novel concealment)</td>
<td>High</td>
<td>High</td>
<td>Medium-High</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>OTHER WEAPON (firearms, knives or blunt instruments used to attack passengers or crew but not to commandeer aircraft)</td>
<td>Low</td>
<td>Medium-Low</td>
<td>Low</td>
<td>LOW</td>
</tr>
<tr>
<td>MAN-PORTABLE AIR DEFENSE SYSTEMS (MANPADS) (in combat or proliferation zone)</td>
<td>Medium-High</td>
<td>High</td>
<td>High</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>MANPADS (not in combat or proliferation zone)</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>VEHICLE-BORNE IED</td>
<td>Medium-High</td>
<td>Medium</td>
<td>Medium-High</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>CARGO IED</td>
<td>High</td>
<td>High</td>
<td>Medium-High</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>LANDSIDE IED (detonated outside security restricted areas)</td>
<td>High</td>
<td>Medium-Low</td>
<td>Medium-High</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>

*Table 1. Threat type risk levels*
7.1 The table above is a compilation of the threat scenario categories that the WGTR has assessed or begun to assess in terms of global risk. A single threat scenario category often reflects several scenarios or sub-scenarios, the details of which can be found in the risk matrices. Likelihood, consequence and vulnerability have been scored on a five-point scale from HIGH to LOW. The general meanings of the scores, in each case, are contained in much more detailed form, along with the risk matrices and an explanation of the rationale of each score, in the longer version of the RCS, available on the ICAO Secure Portal.

7.2 It is important to keep in mind that these risk results reflect the global picture and not a regional or national picture. For example, the threat level has been assessed at the level it exists in most of the world (with the exception of the MANPADS threat, which varies sharply from place to place and so has been assessed at two different levels), and the vulnerability level is assessed as the residual vulnerability existing should a State have implemented all security measures currently required in Annex 17.

8. **RECOMMENDATIONS FOR FURTHER ACTION**

8.1 In the process of conducting its risk assessments and providing updates to the RCS, the WGTR will develop recommendations for further action, whether immediate risk mitigation measures as discussed above or longer-term measures that may be incorporated into Annex 17 or ICAO documents. Further information on the RCS and the applied methodology can be obtained from the Threat and Risk Working Group via the ICAO Secretariat (sfp@icao.int or AVSEC@icao.int).

8.2 **Long term creation and maintenance of risk assessments**

8.2.1 In the longer term, in support of regular updates to the RCS as a living document, the WGTR will continue to develop and update its risk assessments on evolving and unaddressed aviation security threats. The WGTR acknowledges that a risk assessment is a snapshot in time that must be revisited on a regular basis, because any element of the analysis can change and, in particular, as successful or foiled terrorist attacks occur.

8.2.2 States should take into account the RCS as part of their risk-based national civil aviation security programmes.