CIVIL AVIATION AUTHORITY
OF NEW ZEALAND
Te Mana Rererangi Tūmatanui o Aotearoa

Advisory Circular
AC109-1

Revision 6

Regulated Air Cargo Agent – Certification

5 April 2025

General

Civil Aviation Authority (CAA) Advisory Circulars (ACs) contain information about standards, practices, and procedures that the Director has found to be an **acceptable means of compliance** with the associated rule.

Consideration will be given to other methods of compliance that may be presented to the Director. When new standards, practices, or procedures are found to be acceptable they will be added to the appropriate AC.

Purpose

This AC describes an acceptable means of compliance with the security requirements and standards of Civil Aviation Rule Part 109, *Regulated Air Cargo Agent – Certification*[1], for the carriage by air of cargo and mail on an aircraft conducting an international regular air transport passenger service.

Related rules

This AC relates to Part 109. *Regulated Air Cargo Agent – Certification.*

Change notice

Revision 6 updates sections to align with the Civil Aviation Act 2023 (CA Act 2023), and other information on certification requirements to align with CAA's Certification and Licensing policy. It also removes specific form references.

---

[1] Throughout this AC a specific sub-section within a Rule Part will be referenced as 'rule' e.g. rule 109.55.

Published by
Civil Aviation Authority
PO Box 3555
Wellington 6140

Authorised by
DCE Aviation Security and Infrastructure

Version history

The version history is outlined below:

AC Revision no	Effective date	Summary of changes
AC109-1, Rev 0	8 October 2008	Initial issue of this AC.
AC109-1, Rev 1	20 September 2010	Removed reference to actual dollar amounts where CAA fees are mentioned and instead referred to the Civil Aviation Charges Regulations.
AC109-1, Rev 2	22 August 2013	Updated the publication details and the contact addresses on pages 4, 7, 10 and 11.
AC109-1, Rev 3	29 August 2013	Corrected the reference to rule 12.55(d)(8) on page 18.
AC109-1, Rev 4	11 October 2021	Updated email and other addresses and included advice on how to find information on the CAA website. Minor clarifications made and standardised style. Added a version history.
AC109-1, Rev 5	14 February 2024	Expanded advice on the acceptance and ongoing oversight of known customers in New Zealand's air cargo and mail secure supply chain. Added sub-sections to clarify the intent of rule parts. Added a sub-section on the security control of transhipment cargo Added more detail on an acceptable form of compliance for RACAs to ensure their obligations as a Part 109 certificate holder are being met, with particular reference to rule 109.61. Updated the sections on IQA and Occurrence Reporting. Added appendices: • Template for known customer register • Known Customer Security Programme (example) • Security Culture

Published by
Civil Aviation Authority
PO Box 3555
Wellington 6140

Authorised by
DCE Aviation Security and Infrastructure

		• Elements of a strong security culture, and • Transhipment Cargo. Made minor clarifications. Corrected typos and aligns style and format with current AC format.
AC109-1, Rev 6	5 April 2025	Updates sections to align with the CA Act 2023. Updates information on certification requirements to align with CAA's Certification and Licensing policy. Removes specific form references.

Table of Contents

Introduction

The advice in this AC provides practical information for RACAs to support their compliance with Part 109. This includes an acceptable means of compliance for how RACAs can assess and monitor known customers and their procedures, through their security programme.

Monitoring and checks to ensure known customers are meeting security and audit requirements will help provide RACAs with assurance and enable them to demonstrate to CAA that both they and their known customers have systems and checks that are functioning as intended.

***Note**: Only rules requiring compliance guidance and informative/explanatory material are included in this section. Where the rule is self-explanatory, no information is given.*

Subpart A – General

Rule 109.1 Purpose

The requirements of Part 109 apply to cargo and mail being carried by air on aircraft conducting international regular air transport passenger services.

Rule 109.3 Definitions

Relevant definitions for Part 109 are contained in Part 1, Part 12 and rule 109.3. Some key definitions are repeated below for ease of reference, but other definitions are specific to this sector.

Term	Definitions~~:~~
Access controlled	In relation to a particular area, an area that is secured in a manner that prevents the entry of any unauthorised person.
Air operator	The holder of: (1) an air operator certificate granted under section 75 of the CA Act 2023 and in accordance with Part 119, or (2) a foreign air operator certificate granted under section ~~9~~ 75 of the CA Act 2023 and in accordance with Part 129, or (3) an Australian air operator certificate with ANZA privileges.
Authorised person	Someone who is authorised under rule 109.59 to carry out all or any of the security control functions applicable to the RACA's activities.
Cargo	Any property carried on an aircraft other than mail, stores and baggage.
Cargo security incident	An incident involving cargo or mail that is carried, or has been accepted by a regulated air cargo agent or an air operator for carriage, by air on an aircraft conducting an international regular air transport operation passenger service, and:

	(1) there is evidence of tampering or suspected tampering with the cargo or mail which could be an act or an attempted act of unlawful interference, or (2) a weapon, explosive, or other dangerous device, article or substance, that may be used to commit an act of unlawful interference is detected in the cargo or mail.
Declaration of security	A declaration made in accordance with the requirements of rule 109 regarding a consignment of cargo or mail.
Incidents	Events which compromise or impact the integrity and/or security or cargo and or mail, including (but not limited to) potential and/or actual breaches of security.
Known customer	A shipper of cargo or mail who has an established association with a RACA or an air operator for the carriage of the shipper's cargo or mail by air and who is registered with the RACA or the air operator.
Mail	Any letter, package, parcel, postcard, or other article that is to be delivered by courier, a postal operator, or other postal agency, or diplomatic agency.
New Zealand Customs Service (NZCS) Secure Exports Scheme (SES)	A programme that certifies New Zealand exporters who meet NZCS secure supply chain expectations, to help these exporters clear customs. Exporters joining the scheme need to ensure their goods are packed, stored, and transported in a way that meets global customs standards.
Part 109 certificate	A certificate granted by CAA under Part 109, which allows an operator to act as a RACA. In previous revisions of this AC, sometimes referred to as a RACA certificate.
Regulated air cargo agent (RACA)	A holder of a Part 109 certificate granted under section 75 of the CA Act 2023 and in accordance with Part 109.
RACA Certifier	Person responsible for ensuring that the consent form and subsequent on-line application form is accurately completed, the details supplied are legible and the identity of the applicant has been verified.
Searching[2]	The application of technical or any other means to detect a weapon, explosive, or other dangerous device, article or substance, that may be used to commit an act of unlawful interference. ***Note**: Certain dangerous articles or substances are classified as dangerous goods and must be transported in accordance with Part 92.*
Security control	A method used to prevent the introduction on board an aircraft or at an aerodrome, of a weapon, explosive or other dangerous device, article

[2] Note that the term 'searching', not screening, is used in the CA Act 2023.

	or substance that may be used to commit an act of unlawful interference.
Security programme	Policies, records, and procedures which: 1) detail information about a known customer's operation and how they apply security controls and measures, and 2) provide assurance to a RACA that the policies and procedures outlined by a known customer meet the RACA's requirements.
Statement of content	An accurate description of the items that are contained within a consignment of cargo or mail for carriage by air.
Transfer cargo	The movement of cargo from one aircraft to another, without leaving the aerodrome environment, where the cargo remains in the control of an Air Operator.
Transhipment cargo	The unloading of cargo from an aircraft, where it is removed from the aerodrome environment 'under Customs bond' by a RACA and deconsolidated, before re-entering the secure supply chain either in its entirety or as part of a new consolidation.
Transit cargo	An en route stopping place where cargo remains on board an aircraft and in the control of an Air Operator.
Unlawful interference	An act or attempted act endangering a passenger, crew member, ground personnel, aircraft, or facility.
Unknown customer	A customer that has not been registered as a known customer, and whose cargo has not had security controls applied to it.

Rule 109.5 Requirement for certificate

A person must not act as a RACA except under authority of and in accordance with a Part 109 certificate[3].

Rule 109.7 Application for certificate

The application form for issue, renewal, or amendment of a certificate under Part 109 and associated compliance matrices are available on the CAA website - Regulated Air Cargo Agent (forms). The application also needs to include the exposition required by rule 109.71[4] and a completed fit and proper person (FPP) questionnaire required for a senior person identified as

[3] It is an offence to breach this rule – see Civil Aviation (Offences) Regulations 2006 (SR 2006/168) (as at 11 November 2020) Schedule 1 Offence provisions and penalties

[4] For a detailed explanation of what an exposition is and what it should contain, go to the section on rule 109.71 of this AC.

the Chief Executive (CE) and a senior person or persons responsible to the Chief Executive (CE) required by rule 109.51[5].

To find the applicable forms, go to the 'Forms' tab on the CAA website and click on the filter for Part 109.

All documents are to be submitted to the Director of Civil Aviation via the Aviation Security and Infrastructure Unit's Team Coordinator at:

Team Coordinator
Aviation Security and Infrastructure
Civil Aviation Authority
PO Box 3555
Wellington 6140

Email: security.regulation@caa.govt.nz

An application for a Part 109 certificate will not be assessed until all relevant application forms and associated documents are provided in a completed state to CAA. It is recommended that the organisation submits their application in plenty of time so CAA can allocate enough time to assess all the information.

The current charge payable for the assessment of an application for a Part 109 certificate is prescribed in the Civil Aviation Charges Regulations (No 2) 1991 and is available on the CAA website - Charges

Rule 109.9 Grant of certificate

Part 109 certificates are granted in accordance with section 75 of the CA Act 2023. The Director has certain obligations when granting certificates. These include being satisfied that:

(1) the applicant meets the applicable requirements of Part 109

(2) the nominated senior persons in the organisation are fit and proper persons

(3) the exposition includes procedures detailing the organisation's methods of compliance with the relevant rules, and

(4) granting the certificate is not contrary to the interests of aviation safety or security.

Rule 109.11 Privileges of certificate holder

This rule is self-explanatory.

Rule 109.13 Duration of certificate

CAA will undertake a thorough and comprehensive assessment as part of any initial certification process so that the Director is suitably assured that the applicant will meet, and continue to meet, requirements. A Part 109 certificate, granted or renewed by the Director, is valid for a maximum period of up to five years.

[5] For further information about the FPP questionnaire and the Criminal and Traffic Offence history records, including a report from the Ministry of Justice, go to the section on rule 109.51 of this AC.

Note: *To manage workflows, e.g. to prevent delays caused by applications being due just before holiday periods, CAA may grant a certificate for less than five years to ensure CAA assessors can progress applications efficiently.*

Each aviation document has an expiry date. If the holder of an aviation document wishes to continue the activities of the certificate beyond the expiry date, they must apply for a new certificate on the correct form. To find the applicable form, go to the 'Forms' tab on the CAA website, click on the filter for Part 109, then search for 'application for issue, renewal, or amendment of a regulated air cargo agent certificate'.

The renewal application must be made sufficiently in advance of the expiry date to allow CAA to process the application. For further information on the renewal process refer to the section on rule 109.15.

Rule 109.15 Renewal of certificate

It is the RACA's responsibility to be aware of the expiration date on their certificate and when the certificate renewal process should begin.

The RACA must contact the CAA Security Regulation Unit (security.regulation@caa.govt.nz) with an application not less than 30 days before the certificate expires, or earlier if a date is specified on the certificate. CAA strongly recommends that an application is submitted well in advance of this. Applications for renewals should be made before the current certificate expires, as early applications may prevent any issues arising that could delay the issue of the certificate.

The renewal process is a re-entry back into the aviation system. A RACA will need to submit a new application covering all regulatory requirements to meet Part 109. As outlined in rule 109.7, the renewal of a RACA certificate requires all relevant documents to be completed and submitted to CAA.

The time taken to assess a renewal application varies by organisation. CAA's assessment focuses on aviation risk, so assessors consider:

- the nature and scope of the aviation activity
- the type of aviation risks being managed
- how much the operator and their operation has changed
- the operator's previous performance, and
- their attitude towards safety and security

when working out how detailed the assessment needs to be.

Subpart B – Certification requirements

Rule 109.51 Personnel requirements

Senior Persons - Chief Executive (CE)

The CE is the person responsible for the financing and resourcing of the organisation holding the Part 109 certificate. The organisation holding the Part 109 certificate could be the whole organisation or a branch of the parent organisation. In this context the CE is the title given to the person identified in this position for the purposes of certification, rather than the Chief Executive Officer of the parent organisation, or the organisation as a whole.

For example, if company 'A' is a multi-national organisation, the person identified as the CE in the Part 109 certificate may be the General Manager or Air Freight Manager of the New Zealand branch of company 'A'. To meet personnel requirements, this person must be able to make executive decisions about, the financing and resourcing of the Part 109 organisation in New Zealand and ensure the RACA's exposition complies with Part 109.

This person will need to demonstrate during initial application, renewal, and at any other time, that they have the appropriate knowledge to control the organisation.

Other senior persons

Other senior persons are responsible to the CE for ensuring that the applicant's organisation complies with its exposition.

The number of senior persons should be dependent on the size and scale of an organisation. For example, a large organisation could have two or three senior persons, whereas a very small organisation with a limited number of personnel could propose to have all roles held by one person as CE. In this case, the applicant will need to provide assurance and demonstrate how one person can carry out all these roles without security being compromised.

Senior person competency and capability

During the application process CAA will carefully consider the management of conflicts and potential conflicts of interest and the risks associated with concentrating all the responsibilities on a single person. CAA will assess the experience, knowledge, qualifications and attitude of the senior person to gain assurance that they are competent and capable of carrying out all requirements of IQA effectively.

Senior person applicants may show this through demonstrating knowledge and experience, such as evidence of appropriate qualifications, professional organisation memberships, references from members of industry, and a history of successfully completing similar activities in other jurisdictions. The applicant must be able to provide assurance that they have the skills, experience, and time to undertake the role of senior person.

Fit and proper person (FPP) assessment

To meet the requirement of rule 109.51(a), the CE and senior persons involved must be named in the exposition and full details provided with the certification application. CAA will carry out FPP assessments in accordance with section 80 of the CA Act 2023.

All persons exercising privileges under the authority of a document holder, including all nominated senior persons, are required to meet FPP requirements. The persons nominated must be identified on the application form and a completed FPP form submitted for each person. The person's biographical details or *curriculum vitae* should accompany these forms.

When an organisation applies to renew their certificate, they need to include FPP forms for each of their senior persons.

The declaration for an FPP assessment (CAA 24FPPDEC) may be used by senior persons who have met FPP requirements previously, and can attest that there are no changes to their FPP status, i.e.:

- their health status and criminal conviction/ transport offence history is unchanged, and
- they are doing the same role for which they were granted FPP status.

Senior persons whose health status or criminal conviction/ transport offence history has changed, or who have taken on a new role with different scope and responsibilities, need to fill in an application for an FPP assessment (24FPP).

Section 82 of the CA Act 2023 establishes the rights and appeal provisions where an adverse decision is made under the provisions of section 80.

Authorisations – Security check

Senior persons who undertake tasks that require them to be authorised under rule 109.59 will also have to undergo the security check process required under that rule. Further details on this process are provided in this AC in the section on rule 109.59.

Information regarding security check determination and the application process can be found on the CAA website.

Rule 109.53 Facility requirements

At a minimum a RACA's facilities must be capable of:

- providing a secure environment for receiving consignments of cargo or mail
- applying security controls
- securely storing consignments, and
- delivering the consignments to the air operator to:
  - ensure that consignments are not tampered with, and
  - prevent the introduction of any weapon, explosive, or other dangerous device or substance that may be used to commit an act of unlawful interference.

Distinguishing consignments from unknown and known customers

The facilities must be arranged to ensure that the RACA's personnel are able to distinguish between a consignment of cargo or mail from a customer that has not been registered as a known customer, and which has not had security cargo controls applied to it and from a customer that has been registered as a known customer and has applied security controls to its cargo. One recommended method of achieving this is to have storage areas within the RACA's facilities divided, so that a clear distinction is maintained between:

- cargo or mail that has been screened or come from a known customer – 'known or secure cargo', and is clearly labelled

- cargo or mail that has been received from an unknown customer – 'unknown or unsecure cargo' that is also clearly labelled.

Some RACAs may wish to handle and allow an individual consignment of cargo or mail from an unknown customer to move through their premises without issuing a declaration of security. If so, measures must be taken to ensure that such consignments are clearly identifiable from those for which a declaration of security has been issued. For more detail on what this means, see the section on rule 109.55(a)(5) in this AC.

Maintaining security controls

The facilities must also have access-controlled areas for any cargo that has been subject to security controls before it is delivered to the air operator for carriage on board an aircraft. Cargo must not be left in an area that is accessible to the general public for example, situations where cargo is left on open roadways or freight shed car parks that are not fenced and open to the public. Even if the cargo is left for a short period of time, the security controls need to be sufficient to prevent the introduction of weapons, explosives, or any dangerous devices. These security controls should include the cargo being kept under sufficient direct supervision.

Security by design

Physical security controls should be designed to mitigate a range of risks as, given enough time and determination, an unauthorised person can compromise almost any physical security control. Physical security measures should consider the 'Deter, Detect, Delay, Respond, and Recover' model:

- *Deter* – Impede or discourage unauthorised people from gaining access to your facility, by implementing measures that unauthorised people consider too difficult or need special tools and training to get around.
- *Detect* – Implement measures to find out whether unauthorised activity is happening or has taken place.
- *Delay* – Slow down attempts at unauthorised access to enable effective security responses to be activated, by implementing measures to prevent a harmful event happening.
- *Respond* – Effectively act in the case of an unauthorised act within an appropriate timeframe to delay. prevent, resist or mitigate the impacts of a threat or event.
- *Recover* – Take all necessary actions to re-institute and restore operations following an event in a timely manner.

A risk assessment will help a RACA to understand:

- where it might be vulnerable
- what needs to be protected, and
- what mitigations are necessary.

This will also provide assurance to the Director that the RACA understands its risks and is taking the steps necessary to prevent an act of unlawful interference.

Further guidance can be found on the Protective Security Requirements website.

Access to controlled areas at a facility

A RACA must have procedures in place to ensure that all persons who enter an access-controlled area are authorised by the RACA or are accompanied by a person who is authorised. Further details on this process are provided in this AC under in the section on rule 109.59.

Further to this, under rule 109.109, a RACA must not permit a person to enter, and a person must not enter an access-controlled area unless the person holds a valid written authorisation issued in accordance with the procedures required under rule 109.59(b), or the person is accompanied by a person who holds such an authorisation.

The outcome sought by this rule is that cargo or mail is managed in a manner that will ensure its security from the time of acceptance from a known customer or by having security controls applied to it, until delivery to an air operator.

Incident at a facility

The documented procedures in the exposition need to detail the immediate steps to be taken to report to management (who are responsible for the facility) and the appropriate senior person(s) in cases where:

(1) it has not been possible to prevent the access of any unauthorised person to the facility, or

(2) it is suspected that security measures in place may have been compromised, either through general fault or suspected breached access.

The actions detailed need to be appropriate and sufficient to address any risk to cargo or mail and to ensure the integrity of the security controls previously applied to any cargo or mail that was physically present within the facility at the time in question.

If there has been any tampering or suspected tampering of the cargo or mail which could be an act or an attempted act of unlawful interference, the occurrence must be reported to CAA in accordance with the procedures required under rule 109.65.

Rule 109.55 Cargo and mail security control procedures

A RACA must establish security control procedures for consignments of cargo or mail before they are accepted for carriage on board any aircraft engaged in an international air transport passenger service. These procedures must be appropriate for the nature and scale of the RACA's operations and the scope of the services the RACA intends to provide.

In accordance with rule 109.71(a)(9), the procedures required under this rule must be either included in detail in the RACA's exposition or included at an outline level along with information that identifies the specific documentation that contains the detailed procedures in question. The procedures must be acceptable to the Director and should clearly demonstrate how the RACA will achieve the desired security outcomes.

Note: *Where the requirements of a rule concern security-sensitive information, the document where that information is contained will be the National Aviation Security Programme (NASP). RACAs can ask for a copy of the NASP* at the contact details provided in the section on rule 109.7.

Rule 109.55(a)(1) Security controls for cargo or mail received from an unknown customer

This specific requirement includes security controls which need to be sufficient to prevent any weapon, explosive or other dangerous device, article or substance that may be used to commit an act of unlawful interference from being placed on board the aircraft by this means.

Screening

Screening is a form of security control. Acceptable screening methods are listed in Appendix B, section B.1 to Part 109. Standards for the screening of cargo or mail are contained in rule 109.57. Further details on practices and procedures that the Director considers to be an acceptable means of compliance are provided in this AC in the section on rule 109.57.

The special nature of some types of cargo or mail to be transported by air means that they may not necessarily require screening, even if the cargo or mail is from an unknown customer. Information on the categories of cargo or mail that don't need to be screened is security-sensitive and isn't included in this publicly available AC. The RACA must have procedures to ensure any such categories of cargo received by them are still subject to all relevant secure storage, handling and transport provisions of Part 109.

Relevant information for RACA certificate holders is available upon application to the Team Coordinator, ASU, at the contact details provided in the section on rule 109.7.

Rule 109.55(a)(2) Acceptance of consignments from known customers

Where a consignment of cargo or mail is accepted by a RACA from one of its known customers, the consignment must be accompanied by a statement of content that is clearly identifiable and that can be easily traced and verified as originating from the known customer.

The RACA's authorised person accepting a consignment of cargo or mail into the RACA's facility from a known customer must check the consignment for any evidence of tampering. All consignments that are forwarded to RACAs must be protected from tampering during the journey.

Identification of tampering and protection of a consignment

The RACA's procedures for accepting a consignment of cargo or mail from a known customer must include a means for identifying any tampering to a consignment. Rule 109.61 requires that the known customer has appropriate systems and procedures for protecting a consignment of cargo or mail. This protection must be of a standard that will enable the RACA to readily identify any tampering with the consignment.

There are various means for protecting a consignment. The method of protection used by the RACA must be capable of maintaining the secure status of the consignment to prevent any undetected introduction of any weapon, explosive, or other dangerous device, article or substance that may be used to commit an act of unlawful interference.

Each consignment of cargo or mail forwarded by the known customer to the RACA should be protected from tampering or in a state that would display any signs of tampering. As outlined in more detail in the sections on known customers, the RACA and authorised person(s) should know the type of tamper-evident packaging used by each known customer.

Consignment seals

One method of maintaining the secure status of a consignment is to have the consignment sealed. A seal may be on individual cartons/items of freight or encompass a larger consolidated consignment in palletised or other form.

Procedures for the placement of seals on cargo or mail, where appropriate, must be included in the processes established between the RACA and the known customer.

CAA does not prescribe or mandate the use of any particular type of seal. Where a seal is used it must be capable of displaying identifiable evidence of any tampering to the RACA's authorised person who is accepting the consignment into the RACA's facility.

Where a consignment of cargo or mail, by its nature, is unable to be sealed, procedures must be established that allow the RACA to identify whether or not the consignment has been tampered with when received into their facility.

Transportation

The RACA must ensure that any consignment it receives from a known customer has not been subject to any tampering while being transported between the known customer's premises and the RACA's facilities.

A seal affixed to a consignment for compliance with NZCS requirements is considered acceptable for meeting the Part 109 requirements. An applicant for a Part 109 certificate who intends to use the NZCS seal system to meet Part 109 compliance requirements must include a reference to this in their exposition, as required under rule 109.71. A RACA must also provide details of the processes involved in checking the integrity of the seal upon accepting the consignment into the RACA facility. Any such seal will need to be capable of displaying identifiable evidence of tampering, in any individual instance, to the RACA's authorised personnel.

Note: *There is more information about the NZCS SES on the NZCS website at* *https://www.customs.govt.nz/business/export/secure-exports-scheme/*

CAA will assess any seals applied for compliance with any other agency requirements for Part 109 compliance purposes on a case-by-case basis.

Recognition of other government schemes

Where an applicant or RACA identifies other government export schemes or requirements as potentially being in alignment with the desired outcomes of Part 109, a RACA may consider the requirements of those other schemes in their procedures, provided they can clearly demonstrate how those procedures will achieve the desired security outcomes. The RACA must be able to explain to CAA how these schemes or requirements meet and will continue to meet relevant Part 109 requirements.

It should be noted that not all government export schemes, or component parts of those schemes provide the necessary levels of assurance that an act of unlawful interference will be either prevented or detected. One reason for this is that the requirements of other agencies are designed to mitigate different risks, for example, biosecurity risks.

Inspection by other government agencies

Other government agencies, in particular border agencies, may in the course of their duties, need to inspect consignments from known customers and have the powers to do so. The consignment must be restored to a tamper-evident condition after the inspection. A note

should be made of the time and date of the inspection with the name and contact details of the individual and agency concerned.

Documenting procedures

The procedures established with individual known customers for the acceptance of consignments don't need to be individually contained within the RACA's exposition. They may be held on individual files for each known customer but, in accordance with rule 109.71(a)(9)(iii), the exposition must contain an outline of the process involved in establishing the acceptance procedures and information that identifies the specific documentation containing the detailed procedures in question. Further details on these procedures are provided in this AC in the section on rule 109.61(a)(2).

Rule 109.55(a)(3) Check of statement of content

The RACA must have procedures to ensure that the statement of content provided by a known customer for a consignment of cargo or mail is checked by a person who the RACA authorises to do this. This ensures that the statement of content does not list any weapon, explosive, or other dangerous device, article or substance that may be used to commit an act of unlawful interference.

The statement of content must be identified and verifiable as originating from the known customer. The RACA must have procedures to determine that the person presenting the statement of content to the RACA is a representative of the known customer. By way of guidance, this may involve the use of various forms of photo identification when an individual has presented the statement of content in person. If the statement of content is delivered electronically, the individuals approved by the known customer to issue statements of content must be documented by the RACA and available for verification. This can be carried out through the RACA's own procedural documentation.

The procedures established with individual known customers for statements of content do not need to be individually contained within the RACA's exposition required under rule 109.71. They may be held on the RACA's files for each known customer, with the exposition outlining the processes involved in establishing the procedures and, as required by rule 109.71(a)(9)(iii), information on where to find the documentation that explains the detailed procedures in question.

Rule 109.55(a)(4) Storage of cargo or mail in access-controlled area

The RACA must have procedures to ensure that any consignment of cargo or mail accepted by the RACA, and which has had security controls applied to it, is held in an access-controlled area until delivery to the air operator. This includes consignments already loaded for transport.

If a consignment of cargo or mail is removed from the access-controlled area at any time during storage, the RACA must have procedures to ensure the ongoing integrity of the security controls previously applied to the consignment.

Rule 109.55(a)(5) Delivery of cargo or mail to an air operator

Declaration of security

A RACA must have procedures to ensure that every consignment of cargo or mail, handled in accordance with this rule, and delivered to an air operator, is accompanied by a declaration of security.

Where the RACA chooses to allow a consignment of cargo or mail to move through their premises without applying the appropriate security controls, the RACA must ensure that the consignment is not issued with a declaration of security and is identified as unknown cargo to the air operator.

CAA does not prescribe or mandate the use of any format for a declaration of security, but it must contain the information specified in A.1 of Appendix A to Part 109.

A declaration of security must relate to a particular consignment of cargo or mail and must be signed by a person authorised by the RACA under rule 109.59.

The RACA is responsible for maintaining the security of a consignment of cargo or mail from the time the consignment leaves the RACA's access-controlled area until the consignment is accepted by the air operator.

Regulated Air Cargo Agent (RACA) and third-party carriage relationship

If the RACA intends to use a third party to transport the consignment to the air operator, then agreed and documented procedures need to be established (between the RACA and the third party) to ensure that the integrity of security controls applied to the consignment are maintained during transportation to the air operator.

This may include processes that allow for identification of any tampering with the consignment of cargo or mail during the transportation process.

The seal processes referred to above in respect of rule 109.55(a)(2) are also considered an acceptable means of compliance with this rule requirement.

If a consignment of cargo or mail cannot be made tamper-evident for transportation to the air operator, then the transport operation must be carried out by a person who is authorised by the RACA in accordance with rule 109.59(a)(6). Such an authorisation can be issued by a RACA to an employee of a third-party organisation as may be required in such cases, but that employee would require a favourable security check determination by the Director. Further details on the authorisation process are provided in this AC in the section on rule 109.59.

Relevant documented procedures for ensuring that any third-party individual is aware of the RACA's responsibilities for transporting consignments of cargo or mail do not need to be individually contained within the RACA's exposition. The procedures may be held on individual files for each third party, but as required by rule 109.71(a)(9)(vi), the exposition must contain details of the process involved for ensuring that the third party is aware of their responsibilities, including information that identifies the specific documentation containing the detailed procedures.

Security control of transhipment cargo

Transit, or transfer, cargo which does not leave the aerodrome environment remains the responsibility of an air operator in accordance with Part 108.

Transhipment cargo may be accepted as secure (known) provided:

- a copy of the original security declaration is obtained by the RACA
- it is inspected by an authorised person within the RACA to ensure that it is still in its original packaging and that it remains tamper-evident

- there are no anomalies to the original accompanying documentation, including the original security declaration from the point of origin, and
- it is held in an access-controlled area with a copy of the original security declaration retained by the RACA.

If the RACA is not satisfied that the requirements relating to transhipped cargo are met, the cargo must be treated as unknown and further security controls applied.

Any cargo transferring from an all-cargo aircraft to a passenger carrying aircraft must be secured to the standards required by the rule. Where an original security declaration is issued and it is only applicable to cargo-only aircraft, the cargo must be made secure prior to forwarding for carriage on board passenger carrying aircraft.

Refer to Appendix F, *Transhipment Cargo*, for a flow chart of how to assess transhipped cargo.

Rule 109.55(b) Persons implementing security controls

The RACA must ensure that persons implementing security controls required by rule 109.55(a) are appropriately trained and hold an appropriate authorisation issued in accordance with rule 109.59.

For further information refer to the section in this AC on rule 109.63**.**

Rule 109.57 Screening procedures

Rule 109.57(a) Screening procedures

A RACA who intends to screen cargo or mail must have established procedures for such screening. As required by rule 109.71(a)(9)(vii), the procedures required under this rule must be either included in detail in the RACA's exposition or included in the exposition at an outline level, along with information that identifies the specific documentation that contains the detailed procedures.

If a RACA chooses not to screen cargo or mail, this needs to be recorded in the exposition. In such instances where consignments are screened by a third party, the exposition should capture the procedures the RACA intends to use to ensure this screening is carried out in accordance with Part 109. Alternatively, they can be presented at an outline level in the exposition with information to identify the specific documentation containing the detailed procedures.

Rule 109.57(b)(1) Methods of screening

The procedures required under rule 109.57(a) must identify the methods of screening to be used by the RACA. Acceptable screening methods are listed in B.1 of Appendix B to Part 109.

Rule 109.57(b)(2) Processes of screening

Procedures to be followed by each person conducting screening (using one or more of the methods identified in B.1 of Appendix B to Part 109) must be established.

As an example, these procedures may include the need to physically search items of cargo or mail where required, or the application of another method or additional means of screening when an item subject to x-ray screening is unable to be clearly identified on the x-ray monitor.

Any method of screening to be used by the RACA must meet standards that are acceptable to the Director. The Director will consider the ability of any particular screening method to detect

an aviation threat-sized quantity of explosive. A range of factors may impact on what quantity of explosive could be a 'realistic aviation threat' in any particular instance.

When considering the acceptability of any individual screening system or method, the Director may consider any prior acceptance or certification of such a system or method for cargo screening purposes by other international regulatory or technical bodies.

Detailed guidance material on the acceptability of screening methods and procedures is security-sensitive and isn't suitable for inclusion in this publicly available AC. Relevant information for RACA certificate holders is available upon application to the Team Coordinator, ASU, at the contact details provided in the section on rule 109.7.

The documented procedures for the screening method must include procedures for the management of situations involving the detection of any suspected or undeclared explosive device or substance. For more advice on this, refer to the section in this AC on rule 109.65.

Some aspects of the procedures for managing these situations may vary depending upon the physical environment of the individual RACA's premises, the size and nature of the item or consignment in question, and the method of screening being applied at the time. It is also recognised that RACAs may have other compliance requirements that relate to employee health and safety considerations and hazardous substances.

Accordingly, it is neither practicable nor desirable for CAA to specify a procedure that may be applicable in any particular situation. RACAs should ensure that any procedures provide for the safety of RACA personnel, and any other person whose safety may be at risk. This includes alerting Police, and the actions to be taken to ensure that the consignment, or item containing the suspected or actual explosive device or substance, is contained, and the area is cordoned and controlled in a manner that mitigates the threat posed by it.

Rule 109.57(b)(3) Authorisation of screeners

Persons conducting screening must be individually authorised in accordance with rule 109.59. The authorisation must specify what method of screening the individual is authorised to use.

Rule 109.57(b)(4) Periodic testing of screening method

A test of the screening method should be completed periodically, at least once every 28 days, to give ongoing assurance that the method is functioning as required and capable of delivering ongoing and appropriate levels of detection.

The proficiency of the personnel who conduct screening methods should be tested periodically, at least once every 150 days. The testing must be done in accordance with the requirements of B.2 of Appendix B of Part 109.

Detailed guidance material on acceptable testing processes (including acceptable test pieces) is security-sensitive and isn't suitable for inclusion in this publicly available AC. Relevant information for RACA certificate holders is available upon application to the Team Coordinator, ASU, at the contact details provided in the section on rule 109.7.

Rule 109.57(b)(5) Screening equipment maintenance

Technical equipment used for screening must be maintained to high standards to ensure that it remains capable of detecting, in cargo or mail consignments, any weapon, explosive, or other dangerous device or substance that may be used to commit an act of unlawful interference.

Equipment manufacturers will specify a programme of maintenance for the equipment, which will generally be acceptable for the purpose of compliance with this rule. The maintenance programme must be included within the RACA's exposition. This should be either outlined at a level of detail which identifies the documentation and procedures that contain the maintenance programme, or detailed within the exposition itself.

Rule 109.57(b)(6) Screening method failure

If a failure of the screening method is detected, either during a scheduled screening method test or during the screening process itself, the RACA must have procedures in place to assess the extent of the failure. The assessment process must include the procedures and criteria to consider the requirement to recall any consignment of cargo that has been screened but not carried by the air operator at the time the failure is discovered.

If the assessment of the screening method failure determines that cargo already screened and not carried by an air operator requires additional screening, then the RACA must have procedures in place to ensure this additional screening is applied.

Rule 109.59 Authorisation procedures

A RACA must have procedures in place to issue an authorisation to the personnel who are employed by or contracted to the RACA to carry out the security control functions (applicable to the RACA's proposed activities) listed in rule 109.59(a)(1) – (7). To be issued an authorisation, the individual must be:

(1) granted a favourable security check determination by the Director in accordance with section 126 and 127 of the CA Act 2023.

(2) appropriately trained in accordance with the RACA's training programme required under rule 109.63, and

(3) assessed as competent (in accordance with the training programme required under rule 109.63) to carry out the functions for which the authorisation is intended.

Any contracted person working for more than one RACA must be individually authorised by each RACA. The authorisation by each RACA will require the contracted person to have been granted a favourable security check determination by the Director as in (1) above. This check only needs to be completed once, but the contracted person will need to supply each individual RACA with documented evidence that they hold a favourable security check determination before the RACA can issue an authorisation to that person.

The RACA must have a training programme which details how they are going to train their personnel who carry out security control functions, including any contractors and their staff.

Guidance material on the training and competency assessments is contained in this AC at the section on rule 109.63, and at Appendix A of this AC.

An authorisation issued in accordance with rule 109.59 can only remain valid for a maximum period of three years. Any re-issue of an authorisation to a person must be in accordance with rule 109.59(c). This includes a new security check determination by the Director.

Rule 109.59(b) Authorisation to enter an access-controlled area

An access-controlled area is established to maintain a secure environment in which air cargo is stored in the RACA's premises. Therefore, there is a need to ensure appropriate control of persons entering that area.

This rule requires the RACA to have procedures to issue an authorisation to every person who is required to enter an access-controlled area, other than those escorted in accordance with rule 109.109(2), whether to undertake security controls for the air cargo or for any other reason.

The RACA should include procedures to ensure that, in accordance with rule 109.109, persons who are granted permission to enter an access-controlled area are authorised in accordance with rule 109.59(b) or are accompanied by a person who is duly authorised.

Rule 109.59(c)(1)(i) Security checks

An authorisation must not be issued unless the person has undergone a security check and been granted a favourable security check determination by the Director as in (1) in the section on rule 109.59 above. The security check is required to determine whether or not the person poses a threat to aviation security.

Confirmation of identity

Before any authorisation is issued by the RACA, the identity of the person authorised must be confirmed as correct by the RACA. The applicant must complete a RACA security check consent form and give this to their employer's RACA Certifier along with a colour copy of an approved form of identity and any other required documentation as noted below. The RACA Certifier will submit this information to the Airport Gateway portal.

The RACA Certifier is responsible for ensuring that:

- the consent form and subsequent online application form is accurately completed
- the details supplied are legible, and
- they (the RACA Certifier) have verified the identity of the applicant on the form.

Accurate completion of the consent form and online application will assist in ensuring the security checks can be conducted in a timely manner.

The application form will need to be accompanied by a colour copy of one of the following approved forms of identification for the applicant:

- New Zealand driver licence – must be current or expired within the last two years, must show the expiry date and the applicant's signature, must not be cancelled, defaced or a temporary licence, or
- New Zealand passport – must be current or expired within the last two years, must show the applicant's signature, must not be cancelled or defaced, or
- Overseas passport – must be current, must show the applicant's signature, must not be expired, cancelled or defaced, or
- New Zealand firearms licence – must be current, must not be expired or defaced, or
- Certificate of identity – must be current and issued by the Department of Internal Affairs (DIA), or
- Refugee travel document – must be current and issued by DIA, or

- Statutory declaration – must be signed and dated by a Justice of the Peace (JP) or other authorised person, with an accompanying countersigned and dated photo of the applicant.

In addition, copies of the following must be provided, as applicable:

- Permanent resident, resident, work or student visa – if the applicant is not a New Zealand or Australian citizen and they are in New Zealand on a permanent resident, resident, work or student visa.
- Proof of legal change of name (for example a marriage or civil union certificate or a dissolution of marriage or civil union certificate) – if the applicant wants to use a name that is different to the name that appears on their approved form of identification.
- Proof of New Zealand citizenship – if the applicant is a New Zealand citizen who was born outside New Zealand, and they are not providing a copy of a New Zealand passport with their application.

A copy of the confirmation of identity and consent form must be retained by the RACA Certifier in accordance with rule 109.67(a)(3).

Rule 109.61 Procedures and register for a known customers

This rule requires a RACA to:

(1) have procedures in place relating to their known customers and that these procedures deliver the specific outcomes listed in rule 109.61

(2) ensures that these procedures continue to deliver the required outcomes on an ongoing basis, and

(3) maintains a register of their known customers, such as the template provided in Appendix B of this AC.

To achieve this a RACA must review and gain assurance from known customers demonstrating that the security controls and processes they have in place are appropriate and achieve the intended security outcome. This is achieved through validating known customers' systems and procedures.

Validation and revalidation of known customers

The RACA must review and validate the documented procedures contained in a known customer's security programme before accepting the known customer onto their register. When validating, the expectation is that a RACA will visit the known customer prior to acceptance, and at re-acceptance if the known customer is already on the RACA's known customer register. The purpose of the visit is for the RACA to:

- inspect all aspects of the known customer's operation, and
- provide assurance that the security control procedures outlined in the security programme continuously demonstrate compliance with rule 109.61.

CAA expects the RACA to schedule a review with the known customer at an interval of no more than three years, and revalidate the procedures in the known customer security programme. This must also include on-site verification to assess whether the known customer continues to demonstrate compliance with rule 109.61.

The visit must be documented with details of what was inspected, and with whom, from the known customer's staff. In some exceptional circumstances, a remote visit using audio visual conferencing software, such as Microsoft Teams, may be substituted for a visit in person. This will only be acceptable, however, if the RACA:

- can ensure and demonstrate that all aspects of the known customer's operation can be reviewed, and
- documents the results of such an engagement thoroughly.

Remote validation of known customers must not be relied upon as a primary means to verify compliance.

New Zealand Customs Service (NZCS) Secure Exports Scheme (SES) seal system

A RACA may accept consignments for carriage by air from a known customer who is a member of the NZCS SES for shipments by air. In such cases, the RACA may accept them as a known customer, provided that:

- the RACA has a system in place to gain assurance of the known customer's continued membership of the NZCS SES, and
- the RACA has systems and processes in place to ensure that any cargo which arrives does so in a tamper-evident manner, or that cargo which shows signs of having been tampered with is treated as unknown.

***Note**: Refer to the section on Monitoring of known customers.*

In all such cases however, the RACA's exposition needs to document the procedures by which they determine a particular known customer is, and continues to be, a current member of the SES. This includes what steps the RACA takes to monitor the known customer's performance to ensure they continue to comply with NZCS requirements, and how the RACA continues to be assured that any security concerns raised by NZCS that could require a review of the organisation's known customer status are established.

Following acceptance of known customers

To ensure the ongoing integrity of the supply chain, a RACA should maintain positive, rigorous and ongoing oversight of its known customers to meet the requirements of rule 109.61.

Upon acceptance of a known customer by a RACA, the RACA must add that known customer on the RACA's known customer register. For further specific detail on the requirements and maintenance of each RACA's known customer register, refer to rule 109.61(c) *Known Customer Register.*

As required by rule 109.71(a)(9) the procedures by which known customers are recognised by the RACA must be detailed in the RACA's exposition. Details of individual known customers don't need to be specified in the exposition, but the exposition must contain information that identifies specific documentation.

An example of a known customer security programme is provided in Appendix C of this AC. This provides guidance on the types of information required from a known customer and questions that could be asked by a RACA to ensure that the policies and procedures outlined by a known customer meet the RACA's expectations.

Rule 109.61(a)(1) Known customer knowledge of security matters

This rule requires a RACA to establish procedures to ensure their known customer has a comprehensive knowledge of security matters relating to the carriage of their (the known customer's) cargo or mail along the supply chain.

The requirements are to have documented procedures, background checks and training for staff involved in handling air cargo. This information is best provided in a site-specific security programme.

A RACA should provide the format of the security programme to potential known customers and ensure that the guidance has been explained, and clearly understood by, the known customer. A sample security programme is included in Appendix C of this AC which can be adopted for use.

The security matters relevant to the known customer's operations must include the elements of the example security programme in Appendix C of this AC.

Rule 109.61(a)(2) Known customers' appropriate systems and procedures

The RACA must ensure that a known customer has appropriate systems and procedures in place and can demonstrate and provide ongoing assurance that:

1) air cargo is packaged with only the intended items and is stored and prepared for transportation to the RACA in secure areas, and

2) only those with access to cargo or mail and who are responsible for applying security controls can access secure areas, and

3) those personnel that apply security controls to cargo or mail:

    - have undergone a background check that can include (but is not limited to) a Ministry of Justice criminal record check, or evidence of five years' checkable work history with at least two references, considering the suitability of the person to apply security controls to air cargo[6], and

    - are appropriately trained in secure air cargo handling procedures, i.e. having been trained to demonstrate an awareness of aviation security and be competent in any established procedures.[7]

4) there are clear requirements for how a known customer provides the RACA with the name/s and title/s and contact details of the person/s responsible for air cargo security, including the manner and frequency this is supplied, and

[6] In certain circumstances, it may be acceptable for a suitably trained background checked supervisor to oversee the packing process to ensure that only the intended items are included in a consignment. Exceptional circumstances would include when a staff member is unable to obtain a relevant background check (e.g. RSE workers, overseas student workers). The RACA should discuss any other circumstances with CAA, to ensure they qualify as exceptional.

[7] The training programme must also set out how frequently training is to be refreshed and ensure the continued competency of staff is maintained.

5) there is adequate oversight of how security controls are applied, and air cargo and mail is made tamper-evident, and

6) there is ongoing integrity and security of cargo or mail during carriage to the RACA including procedures which ensure cargo and mail will be protected from any unauthorised interference, and

7) known customer procedures are site-specific.

Note: *The RACA and authorised personnel should be familiar with the type and method of tamper-evident packaging used by each known customer.*

The security measures applicable to an individual known customer may vary depending upon the size and nature of their operation and the nature of the cargo they submit for carriage. The method of achieving the above requirements may vary in nature. CAA does not prescribe one method over another.

The outcome sought by this rule is to ensure the security of air cargo as it moves through the secure supply chain.

This requires air cargo to be produced, packaged, stored, transported, and handled in a manner than ensures its integrity and protects it from any potential act of unauthorised interference.

Known customers registered with more than one RACA

A known customer may be registered with more than one RACA. To eliminate the need for duplication, where the established procedures of the known customer meet the requirements of each RACA's exposition on an ongoing basis, the known customer can be registered with both RACAs through the one security programme. This does not, however, remove each RACA's responsibility to ensure they maintain awareness of the ongoing activity of the known customer. Therefore, the means by which compliance is achieved still needs to be included in the exposition.

Statement of content

For each consignment of cargo or mail received by the RACA there must be a statement of content produced by the known customer. The RACA must have procedures to ensure the statement of content has originated from the known customer.

The statement of content must be an accurate description of the items that are contained within the consignment and can be in any form. A commercial invoice or packing slip that accompanies a consignment when shipped are examples of acceptable statements of content.

Rule 109.61(b) Ongoing compliance (known customers)

A RACA's documented procedures must describe how they ensure that the security controls implemented by the known customer continue~~s~~ to meet the requirements of rule 109.61(a)(1) & (2).

The procedures may vary dependent upon the size and nature of the RACA's operations and the nature of the consignments handled.

As an example, they may include reference to:

1) monitoring in the form of random spot checks or targeted audits, with the scope and frequency provided they are determined on the basis of risk

2) documented observations made during visits to the known customer premises by representatives of the RACA, and/or

3) documented observations of methods of tamper evidence and secure transportation.

Monitoring of known customers

Carrying out monitoring

A RACA must regularly monitor their known customers to ensure they continue to meet the requirements of Part 109. A RACA must also be able to explain their monitoring plan to CAA.

To meet the intent of the rules, RACAs need a deep understanding of their known customers and to be able to show CAA how they and their known customers continue to meet all applicable requirements. There are a range of acceptable ways to do this: each RACA's monitoring plan needs to be appropriate to the scale and risk profile of their operation and the known customers they work with.

This gives operators more flexibility to develop plans for monitoring their known customers, but it is also more work, as RACAs have to:

- understand their operation and risks well enough to develop a robust monitoring plan for their known customers, and
- be able to demonstrate and explain to CAA how this plan will work in practice and show that it is rigorous enough to monitor known customers effectively.

For example, a RACA could conduct a random spot check or a targeted audit of a known customer, as long as they are able to explain to CAA how this activity is appropriate to the profile of their operations and the risks presented by the known customer.

Appendix E provides more advice on monitoring known customers, and suggested approaches.

Monitoring can include:

- regular audits
- a special purpose audit – on a particular theme
- spot checks both at the RACA and the known customer
- meetings and interviews with known customers, and
- desktop sampling of paperwork.

In all cases, however, a RACA should:

- maintain strong and ongoing oversight of its known customers
- set expiry dates for known customers, before which the RACA needs to monitor the known customer to ensure it is still meeting security requirements
- maintain its register of known customers
- regularly monitor its known customers to ensure they continue to meet the procedures detailed in their security programmes

- document their monitoring plan and the results of monitoring, and
- monitor each of their known customers at least every calendar year and document the results of this.

Where a RACA identifies issues of known customers not adhering to accepted procedures outlined in the known customer's security programme, the RACA should require the known customer to take corrective action. If monitoring indicates that accepted procedures are not being carried out, corrective action should be put in place using the procedures in a RACA's own quality assurance processes. If accepted procedures are still not being adhered to, the RACA must then:

- remove the known customer from the Register and
- inform CAA, so CAA can inform the wider industry.

Meeting CAA's expectations

When CAA Inspectors assess how a RACA plans to monitor their known customers, they will be asking:

- how RACAs ensure that their known customers procedures continue to meet requirements
- what procedures RACAs have in place to ensure known customers have a knowledge of security matters relating to carriage of their cargo or mail by air, and how that knowledge is maintained
- how the RACA's and known customers' systems and procedures ensure that:
    - only the intended items are contained in the known customer's consignment
    - every consignment is accompanied by a statement of content that can be identified as originating from the known customer
    - every consignment is protected in a manner that enables RACAs to readily identify any evidence of tampering
    - tampering does not occur for consignments sent by the known customer to the RACA, and
    - details held on the RACA known customer register continue to align with the known customer's current information.

As part of this approach, CAA Inspectors will focus on trying to understand HOW a RACA is doing these things, rather than the RACA saying they are in place, without any further explanation. The aim is to understand:

- what training a RACA is running for its staff and known customers, and why this method and frequency was chosen (rather than just being satisfied with the RACA saying that training is done)
- how RACAs decided the methods they chose to monitor their known customers (rather than just accepting that RACAs have got something in place)
- how RACAs keep contact and set expectations with their known customers, and why these methods were chosen.

A RACA has to be able to explain why their procedures and methods were assessed as being suitable and rigorous enough to meet the requirements of their operations and that of their known customers. Where required, inspectors will seek evidence to verify statements made.

Rule 109.61(c) Known customer register

A RACA who intends to accept cargo or mail from known customers must establish and maintain a register of its known customers and have procedures in place to maintain and update this register regularly, or when the RACA is made aware of any changes to a known customer.

The details must include those required in rule 109.61(c). For consistency and accuracy, the template like that provided in Appendix B of this AC should be used by all RACAs for their known customer register.

This register can be kept in manual or electronic form but must be readily available to employees of the RACA who are authorised to accept air cargo or mail from known customers.

When appropriate CAA will review copies of RACAs' known customer registers.

Removal of known customer from register

Should a RACA remove a known customer from their known customer register because the applicant has consistently failed to meet the known customer requirements, the RACA is required to inform CAA by using the Report an Occurrence – Regulated Air Cargo Agents form.

A procedure should be established to ensure that personnel who are responsible for accepting air cargo or mail from known customers are made aware that a particular known customer has been removed from the register.

Rule 109.63 Training of personnel

The training requirements apply to RACA personnel who:

(1) have access to a consignment of cargo or mail that has been accepted by a RACA for carriage by air, and

(2) carry out a security control function in relation to cargo or mail that is accepted by the RACA for carriage by air and who require an authorisation to do so under rule 109.59.

Any training required under this rule is to be carried out by a security instructor who has demonstrated competency to the satisfaction of the CE, or a person nominated by the CE.

The scope of initial and recurrent training needs to be identified and tailored for the different categories of personnel involved in the application of specific security measures contained in the RACA's exposition.

Appendix A of this AC provides guidance on the content of the training and competency levels required for all personnel who have access to air cargo within a RACA's access-controlled area or who are involved in the application of security controls, other than screening, for the RACA.

This material is not an exhaustive list but provides guidance to facilitate compliance with the syllabus content and competency requirements for training required under this rule. Should a RACA desire to provide further training this is encouraged.

All personnel involved in screening functions must, at a minimum, be trained in the specific areas set out in Appendix C to Part 109 and achieve the specific competencies as listed there.

Personnel who undertake security control functions for the RACA must be assessed to be competent by the trainer before the person undertakes a particular security control function for which they are deemed competent.

Recurrent training, as required under rule 109.63(c) must not exceed three-year intervals and should include regular interim refresher training on basic elements and instruction on:

(1) changes to the threat factor affecting the organisation's operations

(2) changes in regulatory requirements and standards, and

(3) changes to the organisation's procedures and programme.

In addition to the training requirements prescribed in Part 109, the RACA needs to be aware of the responsibilities referred to in[8] Section 13(4)(b) of the CA Act 2023 regarding training and supervision of employees.

Where there has been a change to a RACA's procedures that may affect day-to-day operations, staff must be made aware of the change.

Rule 109.65 Cargo security incidents

Rule 12.55(a)(8) makes the reporting of serious cargo security incidents mandatory, but, as noted below, CAA encourages RACAs to report all security-related concerns.

The incidents to be reported include those where:

(1) there is evidence of tampering or suspected tampering with the cargo or mail which could be an act or attempted act of unlawful interference, or

(2) a weapon, explosive, or other dangerous device, article or substance that may be used to commit an act of unlawful interference, is detected in the cargo or mail.

Information required for notification purposes is specified in *Part 12, Appendix A, Information Required for Initial Notification of Incidents*, para (h), *Cargo security incident*: including:

(1) date and time of the incident

(2) a brief description of the nature of the incident

(3) details, if known, of where the incident may have occurred, and

(4) the name, organisation, and contact details of the person notifying the incident.

The RACA must have procedures to investigate the incident and implement corrective action to eliminate the cause of the incident, then put in place preventive action to stop the incident reoccurring.

[8] Section 13(4)(b) states that 'An aviation participant who holds an aviation document that authorises the provision of a service within the civil aviation system must provide training and supervision to all employees of the aviation participant who are doing anything to which the document relates, so as to maintain compliance with the relevant prescribed safety and security standards and the conditions attached to the aviation document and to promote safety and security…'

Specific guidance material on the requirements for notification and investigation of incidents can be found in AC12-1, *Mandatory occurrence notification and information,* and AC12-2, *Occurrence Investigation*, which are available on the CAA website: www.caa.govt.nz under the tab Advisory Circulars.

Reporting concerns to CAA

CAA encourages reporting of all security-related concerns, even when these may not reach the formal requirements for reporting under Part 12. Among other reasons, this is because details of security occurrences help CAA identify threats or risks to the aviation sector.

RACAs are strongly encouraged to use the Report an Occurrence – Regulated Air Cargo Agents form to voluntarily report any security incident or concerns to the Security Regulation Unit.

Incidents or concerns include:

- suspicious interactions
- observations of security concern, or
- anything else that makes you feel uncomfortable.

Once received, the form will be assessed and assigned to a member of the Security Regulation Unit who may contact you.

Rule 109.67 Records

A RACA must have procedures to manage records required for a range of purposes specified under this rule. The procedures, as required under this rule, must be either detailed in the RACA's exposition required under rule 109.71 or included in the exposition at an outline level, along with information that identifies the specific documentation that contains the detailed record-keeping procedures in question.

Records may be kept in hard copy or electronic form. They must be retained for the periods specified in the rule.

Personnel records must include those relating to all persons authorised by the RACA under rule 109.59. These records are to include the training undertaken by the individuals and a copy of the favourable security check determination relating to them. The records must contain the information required by this rule and be retained for the periods specified in rule 109.67(b).

Rule 109.69 Internal quality assurance (IQA)

The purpose of IQA is to provide assurance to the RACA CE and senior persons that the organisation is in compliance with its exposition, its security objectives, and all the applicable rule requirements. It also provides assurance that errors and mistakes are quickly identified and addressed.

IQA is not an optional extra, or afterthought, but an integral part of how a RACA goes about its business. It is recommended that a RACA's IQA system be established with:

- A security policy outlining the organisation's commitment to implementing procedures.
- An audit programme, determined on the basis of risk presented and size/scope of the operation.

- Procedures to ensure that quality indicators, including security incidents, staff and customer feedback, are monitored to identify problems and prevent causes of problems.
- Procedures for corrective and preventive actions, including some form of causal analysis to determine the root cause.
- A management review to ensure the continuing suitability and effectiveness of the quality assurance system. See Appendix D, Security Culture, in this AC for further guidance.

These are the basis for developing quality management and IQA processes that are:

(a) continual, incorporating the techniques of inspections, audits, and reviews to assess the adequacy of managerial controls in key programmes and systems

(b) ongoing, identifying deficiencies, developing corrective action plans to correct these deficiencies, and performing follow-up reviews, and

(c) independent, with straight-line reporting responsibility to top management.

The complexity of these processes depends on the scale of a RACA's operations, but CAA would expect a CE or senior person to be able to explain how decisions were reached about the scale, scope and frequency of IQA activities.

CAA encourages organisations to extend their IQA procedures beyond regulatory compliance to determine the causes of other deficiencies in company operations. From these determinations the necessary enhancements to company operating practices can be made before deficiencies occur or mistakes happen.

Guidance material on the requirements for an internal quality control process can be found in AC00-3, *Internal Quality Assurance*. It may also be helpful to refer to ISO 9001 manuals .

The senior person responsible for IQA is required to have a direct reporting responsibility to the CE for all IQA matters in relation to the security of cargo or mail.

This senior person could delegate responsibility to other staff for their day-to-day duties, but the company organisational structure must show this senior person as having the ability to report directly to the CE on IQA matters.

In organisations with small management teams, consideration must be given to how the IQA and quality management functions can be carried out with enough independence to be thorough and effective.

Rule 109.71 Organisation exposition

General requirements

The primary purpose of an exposition is to express the CE's requirements for the conduct of the organisation and state how the organisation will meet the regulatory requirements. It sets out the procedures, means and methods of a certificated organisation. While there are no ACs about expositions for RACAs, AC139-2, *Aerodrome certification exposition,* has some general advice about how to draft and organise an exposition, what methods can be helpful and who needs to be provided with copies. This can help a RACA develop a useful document that sets out how the RACA will operate, its principles and standards and how it will maintain them.

The exposition is the means by which an organisation defines its operation and shows its employees, its clients and CAA how it will conduct its day-to-day business and ensure compliance with the rules.

An exposition should commence with the corporate commitment by the CE. The remaining parts of the exposition may be produced as any number of separate procedures, sections or as one simple document depending on the extent of the operations proposed.

Depending on an organisation's structure and size, the parts of the exposition could be arranged as:

- Management Policy
- Operations
- Training
- Quality Assurance.

Senior persons should hold copies of those parts of an exposition that affect their area of responsibility, and staff must be familiar with those parts of an exposition that affect their area of employment.

Rule 109.71(a)(1) Corporate commitment

In the organisation's exposition the statement by the CE is a corporate commitment by the organisation. It should clearly state the goals and objectives of the organisation and how it will meet the requirements prescribed by Part 109, for example screening requirements. It may also cover the organisation's goals and objectives in respect of its commercial activities. This is a high-level statement about how the organisation plans to operate and meet its legal requirements: the details of how this will be achieved will be outlined in other parts of the exposition.

Rule 109.71(a)(2) & (3) Senior Persons

The titles and names of the senior persons within the organisation must be listed in the exposition. Their duties and responsibilities, and the areas in which they are directly responsible for liaison with the Director, must be clearly defined. The section in this AC on rule 109.51 provides more detail on senior persons.

Rule 109.71(a)(4) Organisation chart

There must be an organisation chart that clearly details reporting lines, including the lines of responsibility from all senior persons to the CE. The exposition must show the staffing arrangements at each place where the organisation intends to carry out security control functions relating to air cargo and mail.

Rule 109.71(a)(5) Staffing structure

This is a summary of staff at each location. It does not require the names of individuals but should identify staff numbers and role types for all functions and operations that are to be conducted.

Rule 109.71(a)(6) Scope of operations

The organisation needs to identify:

- each location or site where it intends to operate, and
- for each location, the scope of activities that are planned for that location, and
- any functions or roles it intends to contract out, such as applying security controls to unknown air cargo, and
- who the contracted activities will be contracted out to, and
- how the organisation will oversee and monitor the work of contractors.

Depending on the scale and scope of the organisation, a separate diagram showing each site, who will work there and what activities will be carried out there, might be an effective way of showing this.

Rule 109.71(a)(9) Detailed procedures

The procedures should accurately describe the organisation's practices related to its operations. These should either be the detailed procedures, or if the exposition points to other documentation which contains the detailed procedures, include an outline with a brief description of the procedures.

The applicant or RACA should have an effective document control system in place that ensures only current documentation is used, and any material that is obsolete is removed from service. The same level of document control should be applied to an exposition.

Rule 109.71(a)(10) Controlling, amending and distributing the exposition

The exposition must have procedures to ensure that any amendments to, and distribution of, the exposition are controlled. These procedures should detail who amends the exposition, how it is amended and how it is distributed. The front of the exposition should have an effective document control structure in place including a list of affected pages, a record of amendments and a distribution list. These pages are in addition to a table of contents, as they provide a record of what has been changed, when it was changed, and who copies of the exposition have been distributed to.

If a proposed change to the exposition falls within the scope of rule 109.105(b) then the organisation must notify the Director prior to the change, unless this is genuinely not possible. In any case the change must be accepted by the Director.

All other more routine amendments to an exposition must be notified to the Director as soon as practical after the amendment in accordance with rule 109.105(a).

Rule 109.71(b) Acceptance of exposition by Director

RACAs are responsible for their organisation's exposition. It should be a true and accurate description, relevant to their operations, and clearly written.

The acceptance of an organisation's exposition by the Director is part of a RACA's certification and recertification. Unless the Director accepts an exposition, a certificate cannot be issued. The exposition (including any amendments) must remain acceptable to the Director.

Subpart C – Operational requirements

Rule 109.105 Changes to certificate holder's organisation

The RACA is required to notify the Director of any change to the CE or the senior persons, as defined in the rule. The change must be acceptable to the Director before being incorporated into the certificate holder's exposition.

The intention of this rule is not for the Director to approve the change of these people per se, which is an employment matter, but to approve the process of the change and approve the new person or people coming into those roles.

For example, if the CE resigns, the organisation must notify the Director along with an explanation of how this change is going to be managed. The Director may impose conditions on the certificate holder's operations, if required, until a new CE is appointed.

The new CE must meet FPP requirements and any other applicable requirements to be considered acceptable to the Director. This also applies to a change in any of the senior persons listed in the exposition.

Rule 109.107 Persons to issue declaration of security

All persons who issue a declaration of security must hold a valid written authorisation from the RACA. Under the Civil Aviation (Offences) Regulations (2006) issuing a declaration of security without meeting the requirements of rule 109.107 carries a maximum penalty not exceeding ~~of~~ $10,000 for an individual and $50,000 for a body corporate.

Rule 109.109 Entry to access-controlled area

A RACA must not permit a person to enter an access-controlled area unless that person:

(1) holds a valid written authorisation issued in accordance with the procedures required under rule 109.59(b), or

(2) is accompanied by a person who holds an authorisation referred to in paragraph (1).

Requirements for ensuring that the access-controlled area is maintained in a secure manner are covered in this AC in the section on rule 109.53.

Under the Civil Aviation (Offences) Regulations (2006), penalties relating to a breach of this rule are fines not exceeding $10,000 for an individual and $50,000 for a body corporate.

Appendix A – Training guidance material

This appendix provides guidance material on the content of the training and competency levels required for all personnel who have access to air cargo within a RACA's access-controlled area or are involved in the application of security controls, *other than searching*[9], for the RACA. All *personnel involved* in screening functions must, at a minimum, be trained in the specific areas set out in Appendix C of Part 109 and achieve the specific competencies listed there.

This material is not an exhaustive list but provides guidance to facilitate compliance with the syllabus content and competency requirements for training required under Part 109. Specific training necessary for compliance purposes may vary with reference to the nature and scale of the RACA's operations and the scope of the services they intend to provide.

Should a RACA desire to provide further training, this is encouraged. See also Appendix D of this AC.

A suggested means for a RACA to establish that an individual has reached the levels of competency suggested for each topic is to ensure that each individual sits a written examination at the end of their training. Any such examination would need to be under the supervision of the organisation's security instructor referred to in this AC in the section on rule 109.63.

Competency Levels

The levels of understanding and associated competence required to meet rule 109.63(b)(1)(iii) for each of the topics listed below is:

(1) grade 1 denotes awareness of the subject

(2) grade 2 denotes a basic knowledge of the subject

(3) grade 3 denotes the ability to apply a basic knowledge of the subject in a situation that is likely to arise in the course of the person's duties

(4) grade 4 denotes the ability to apply a thorough knowledge of the subject in a situation likely to arise in the course of the person's duties, and

(5) grade 5 denotes the ability to apply a thorough knowledge of the subject and to exercise sound judgement in situations likely to arise in the course of the person's duties.

Security awareness training for staff who have access to air cargo within a RACA's access-controlled areas

(a) Objectives and organisation of aviation security

Staff should be competent to a level of grade 2 and be able to:

- describe the types of people who may pose a threat to civil aviation

[9] Note that the CA Act 2023 refers to 'searching' not 'screening'.

- explain why civil aviation is an attractive target for terrorist groups and others in attempting unlawfully to interfere with civil aircraft
- outline CAA's responsibilities of in relation to security of air cargo
- state why air cargo activities are vulnerable to attack, and
- write an incident report and know to whom it should be sent.

(b) Principles of air cargo security control requirements

Staff should be competent to a level of grade 3 and be able to:

- state the overall objectives of the security controls measures relating to air cargo
- explain the difference in security control procedures for consignments from known and unknown customers (rule 109.55)
- explain the differences in internal company procedures for handling cargo from known and unknown customers, and
- state the RACA's responsibility and obligations in relation to Part 109.

(c) Access control and air cargo protection

Staff should be competent to a level of grade 4 and be able to state:

- the purpose of access control and cargo protection
- the methods of access control and cargo protection used by the RACA (rule 109.53), and
- who to contact in the event of a problem.

Training for staff implementing security controls

(a) Objectives and organisation of aviation security

Staff should be competent to a level of grade 3 and be able to:

- describe the types of people who may pose a threat to civil aviation
- explain why civil aviation is an attractive target for terrorist groups and others in attempting unlawfully to interfere with civil aircraft
- outline CAA's responsibilities in relation to security of air cargo
- state why air cargo activities are vulnerable to attack, and
- write an incident report and know to whom it should be sent.

(b) Principles of the air cargo security control requirements

Staff should be competent to a level of grade 5 and be able to explain:

- the difference in security control procedures for consignments from known and unknown customers (rule 109.55)

- the procedures within the company for handling cargo from known and unknown customers
- the requirements of rule 109.55 in relation to acceptance of air cargo from known and unknown customers
- the requirements of rule 109.61 in relation to the systems and procedures implemented by the known customers, and
- procedure for the issue of a declaration of security (rule 109.107).

(c) Access control and air cargo protection

Staff should be competent to a level of grade 5 and be able to explain:

- the purpose of access control and cargo protection
- the methods of access control and cargo protection used by the RACA (rule 109.53)
- the key responsibilities of staff ensuring access controls are applied, and
- the action to be taken in the event the access controls are circumvented.

Appendix B – Template for known customer register

The template provided below should be used by all RACAs when setting up and maintaining a known customer register. The information contained in the register is the minimum level of information required in order to ensure consistency across the RACA system.

Legal name of entity	Trading name	NZ business number	Address	Registration date	Certification expiry date	Contact name	Phone	Email

Appendix C – Known customer security programme

The template below is an example of a security programme template that RACAs can adopt to assess and monitor known customers:

KNOWN CUSTOMER SECURITY PROGRAMME	
Organisation, security policy, and responsibilities	Key questions a RACA could ask a known customer to be satisfied the procedures/policies meet their requirements.
a) Known customer organisation	*Explaining how your organisation is arranged helps to show how security will be communicated and how different teams work together to achieve security outcomes.* • Is the organisation governed directly by the owners or does it have a board of directors or a committee? • Outline the size and scope of your organisation • Outline the location of your organisation, and any other sites where known customer activities are run from • Is the organisation part of a larger, parent organisation? • Are there any other organisations involved? • What is your organisation's operational structure, e.g., a head office and sub-branches, and how do they work together? • Is your organisation part of the logistics chain in a larger business?
b) Security policy statement outlining organisational	*An organisation's security programme makes a commitment about their organisation's approach to security to by turning it into something tangible. This section aims to uncover how an organisation's security programme is planned and works in practice.*

commitment to implementing Part 109 procedures	• What is your organisation's security policy statement? • How does this statement reflect how your security culture works in practice? • What does being 'security conscious' mean to your organisation? • How would you describe your security policy statement in your own words and in a way that reflects your organisation? • What are the principles that set the rules that you and your organisation will act by? • What are the goals that will turn your security policy statement into a set of accomplishments that the organisation works towards?
c) Known customer's activities and responsibilities relating to aviation security and the secure supply chain	*Describe your organisation's activities and responsibilities in the secure supply chain at a high level.* • Roles involved in all aspects of export air cargo: Manager, Supervisor, Packer, Driver • Locations of your site/s • Locations of any other sites where cargo or mail is securely packaged for transit to a RACA ***Note**: Known customers need to outline responses for all sites where cargo and mail is packaged for a RACA. If the size and scope of the known customer is complex the known customers should consider producing additional security programmes for each site. The expectation is that each known customer has a security programme/s that cover all areas where cargo and mail is packaged for carriage on aircraft.*
d) Role/s responsible for air cargo security	*Detail the roles involved in all aspects of export air cargo at each of your sites.*
e) Policies, procedures, and documentation control systems and how they are communicated to staff	*Outline how staff involved in the export of air cargo and mail understand what they need to do to perform their role.* • How is that information is communicated to them? E.g., Policy documents, overarching policies and plans, are documents controlled, reviewed, and kept up to date?

	• Procedural documents, e.g., task lists, procedures and processes for specific roles, operational manuals, be controlled and kept up to date?
f) Procedures for notifying changes to a RACA to ensure the known customer's security procedures remain current, effective and in compliance with Part 109.	*How does your organisation provide procedures to your known customers?* *How does your organisation assess potential known customers as suitable and secure enough to be accepted as a known customer?* *How does your organisation ensure that any changes to a known customer organisation that impacts how air cargo and mail is prepared for you is notified to your organisation as soon as practicable? This includes changes to operations, security controls, structure.* *What processes do you have in place for updating your known customer register?*
Air cargo and mail security measures	
g) Physical and technical security controls that protect the known customer's sites and facilities, including (but not limited to) detection and surveillance systems	*What security controls are in place to protect a known customer's site from unauthorised access?* For example: • physical • technological • environmental security controls • third-party security services, e.g., security guards, CCTV, and alarm monitoring services • access control on doors • staff identity cards.

h) Production, assembly, packing, storage, and transport:	
i. Measures applied during the production, assembly, packing and storage stages to protect goods to be transported by air from unauthorised interference.	*What procedures are in place at each stage to prevent the introduction of an assembled improvised explosive device (IED) or other foreign object into air cargo or mail?*
ii. Measures applied to secure the goods after packing, including the use of tamper-evident seals.	*What tamper-evident methods are used to package air cargo and mail?* *What is the process of making cargo tamper-evident? Does it specifically cover all sides of the packaging?* *How do these provide the RACA with assurance, and to assess whether it has been tampered with during its journey?* *If tamper-evident security tape, seals or other unique methods are used to make cargo and mail secure, what is the known customer's procedure for storing these at their facility?*
iii. Measures applied to secure the goods for being transported	*What procedures are in place to prevent the introduction of an assembled IED or other foreign object while the cargo is being prepared for transportation?*
i) Access control procedures for air cargo and mail.	*What are the access control procedures for the secure storage of cargo and mail at the known customer facility?* *Do the procedures include physical guarding of the secure storage?* *Is the secure storage area monitored with CCTV?*
j) Measures to keep unsecure cargo from secure cargo.	*Is unsecure and secure cargo kept in separate locations at the known customer facility?* *What other measures are used to clearly identify cargo and mail that is secure from unsecure cargo and mail? For example, coloured stickers.*

k) Documentation:	*Provide an overview of the documentation used through the end-to-end process of delivery of cargo and mail from the known customer to the RACA. What format are the documents?* For example, physical copies or electronic format.
i. Statement of content and other security information relevant to consignments.	*How are packing lists and statements of content generated?*
ii. Measures for documentation control, and record-keeping policies and procedures.	*How are the creation and production of packing lists and statements of content controlled?*
iii. Measures to control access to documentation, records and data to protect information from misuse and alteration.	*What controls are placed on known customer's documents to ensure they are protected?* For example, password protection, encryption, restricted access controls.
Transport	
l) Information on how often and by what method cargo is transported from the known customer to the RACA	*How frequently is air cargo and mail transported to the RACA?* *How is air cargo and mail transported to the RACA?* Is it transported via the known customer's own company, a third-party contractor, or by the RACA themselves?
m) Measures to ensure that air cargo and mail consignments are secure when they leave the known customers premises.	*What security controls are used to ensure the vehicle is secure upon leaving the known customer's premises?*
n) Measures to ensure vehicles remain secure during transport.	*What measures are in place to ensure that vehicles remain secure during transport from the known customer through to the RACA?* *If there is a problem during transportation to the RACA how is this identified and escalated to the RACA for action?*

o) Measures applied to secure the goods while being transported	*What procedures are in place to prevent the introduction of an assembled IED or other foreign object while the cargo is being transported?*
p) A procedure to ensure that the driver is aware of the measures set out in (p) and (q) above.	*What training and procedures are provided to the driver responsible for the secure transportation of air cargo and mail to the RACA?*
Recruitment of staff	
q) Measures to determine all staff are reliable and of good character, through a background check	*What background checks does your organisation perform for prospective new staff and contractors?* *What arrangements does your organisation have in place for the supervision of untrained or probationary staff?* Background checks can include (but are not limited to): 1. A Ministry of Justice criminal record check, or 2. Evidence of five years' checkable work history with at least two references. These checks are required for considering the suitability of the person to apply security controls to air cargo and mail. Any other arrangements concerning the supervision of untrained staff must be discussed with the RACA.
Training of staff	
r) List of roles and personnel involved in the packing, storage, and transportation of cargo.	*List these roles: this could be provided as a separate spreadsheet or as an appendix to the security programme for ease of updating.*

s) Security training programme outline and maintenance of training records.	*What information does your organisation's security training programme include?* *How are training records stored and how long are they retained?* *How is this initial training (at the time of employment) delivered, documented, and recorded?*
t) Initial and recurrent training programmes for:	*What frequency is recurrent training delivered to staff?*
i. Personnel who carry out security measures relating to the packing, storing, and transportation of cargo and/or mail. ***Note:*** *Training materials should be reviewed and refreshed at least every three years.*	*What roles require recurrent security training?* *How is this training delivered, documented, and recorded?*
ii. Staff with access to secure air cargo and/or mail and security awareness training ***Note:*** *RACAs should consider providing security awareness training. This could be through a briefing, for example a power point presentation or video*	*How does your organisation use the security awareness training provided by the RACA?* *What roles and/or areas within your organisation receive security awareness training?* *How is this training delivered, documented, and recorded?* *What frequency is this training provided?*
Reporting of security concerns	
u) Procedures by which known customers will report to the RACA suspected or confirmed cargo and mail incidents of a security nature involving cargo or mail.	*What procedures does your organisation have implemented to report security incidents to RACAs?* *What does your organisation consider a suspected or confirmed security breach and/or incident?*

Appendix D – Security culture

A strong security culture is crucial in preventing the introduction of an assembled IED into the Secure Supply Chain and on to an aircraft.

Continually evolving and increasingly sophisticated threats mean that mitigation has to involve stakeholders throughout the entire Secure Supply Chain.

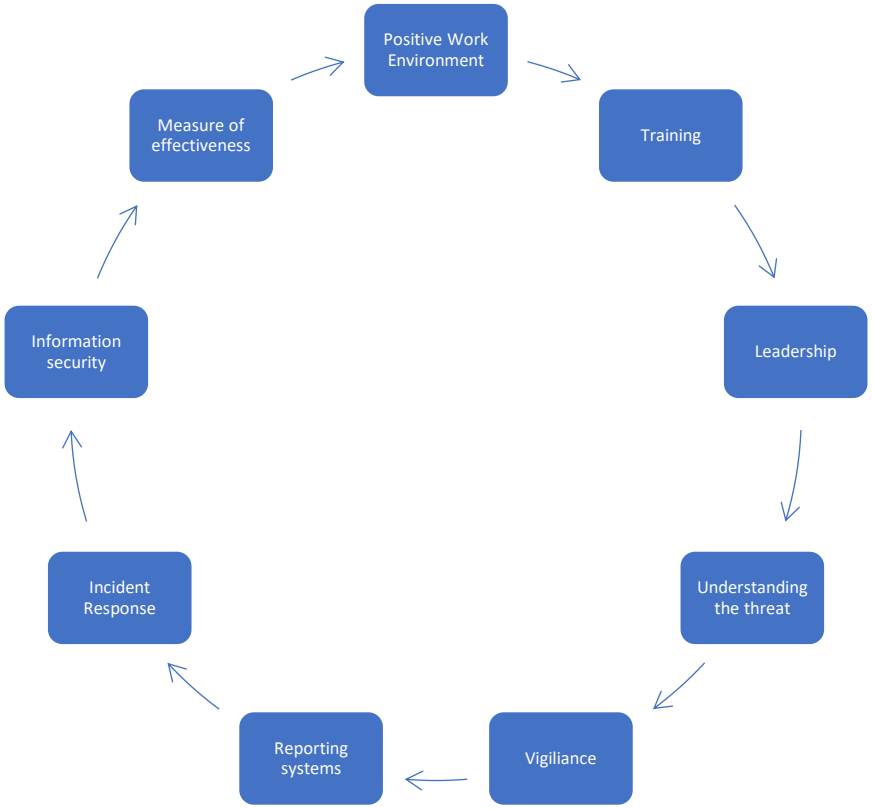
Everyone in the Secure Supply Chain, from known customers through to the RACA to the Cargo Terminal Operator and on to an aircraft, plays an important role in ensure that security measures remain consistent and effective.

Depending on the size and scale of your organisation, you may not need a complicated system to embed an effective Security Culture. You do, however, need to plan and consider which steps and processes will work for your organisation.

In its simplest form, Security Culture means that any suspicious activity is reported:

- See it.
- Hear it.
- Report it.

Figure 1: Security Culture – the different and interlocking elements



Elements of a strong security culture

Any security culture contains different elements, as mapped out in Figure 1:

- **Positive Work Environment –** Are staff encouraged to speak up and provide feedback? Is there a good line of communication between shop floor and management? Is there a No Blame Culture?

  Managers need to be aware of these factors and how the organisation's culture might influence staff willingness to be alert for and report incidents.

- **Training –** At the very least people need to know who to tell if they see something suspicious. Training in this can be provided in a briefing, or by using security culture posters available from CAA by emailing security.regulation@caa.govt.nz

- **Leadership –** Managers should set an example, supporting those who report incidents, and challenging poor performance.

- **Understanding the Threat** From a security perspective, the threat is an assembled IED. However, RACAs might also wish to study the risks posed by Dangerous Goods.

- **Vigilance –** RACAs might wish to encourage vigilance by testing access controls and providing rewards for good security behaviours.

- **Reporting systems –** The management team should create a reporting system with simple methods by which staff can:

  - report suspicious activity
  - suggest improvements,
  - and raise concerns

  and management can use to generate reports. This can be as simple as a mobile phone number. The key is that if people see something suspicious, they need to know who to report it to. Part 109 obliges RACAs to collate and monitor Quality Indicators. These include security incidents, staff feedback and customer feedback.

- **Incident Response –** CEs should have plans for responding to potential incidents. What would a RACA do if someone suspicious was found in the warehouse, or what appeared to a be an IED in cargo?

- **Information Security –** Is information regarding the transportation of air cargo through the secure supply chain kept securely?

- **Measures of Effectiveness –** Once a system has been established, make an effort to measure its effectiveness through the reports received. This will allow you to encourage further attention to security culture if required. As a minimum, Security Culture should be an agenda item for management reviews.

Note: *For the latest information and advice on how to foster a strong security culture, check out the CAA website at: Enhancing your organisation's security culture \| aviation.govt.nz*

Appendix E – Monitoring known customers

Approaches

A RACA should maintain strong and ongoing oversight of its known customers. This is achieved by:

- Setting expiry dates for known customer registration
- Maintaining its register of known customers, and
- Regularly monitoring its known customers to ensure they continue to meet the procedures in their security programmes.

These actions contribute to the effective performance of the secure supply system with respect to the security outcomes we are all seeking to achieve.

RACAs can take one of two broad approaches to monitoring:

1. A commitment to carry out set activities on a regular basis set out in its exposition, or
2. A targeted programme of monitoring activities based on a risk assessment and taking into account:
    - Domestic and international security environments and trends
    - Attractiveness of their business as a target
    - Local events that might increase attractiveness as a target
    - Amount of cargo they process and transport, and/ or
    - Any previous issues in the known customer's operations, e.g. security incidents; issues with staff.

What is monitoring?

Monitoring can include:

- Regular audits
- Special purpose audit – on a particular theme
- Spot checks both at the RACA and the known customer
- Meetings and interviews with known customers
- Interviews with staff of known customers, and
- Desktop sampling of paperwork.

Results of monitoring must be **documented.**

Frequency and handling non-compliance

- Monitoring should take place at both the **RACA and the known customers' locations of work.**

- In any calendar year, **every known customer on the Register must be covered as part of a Monitoring regime.**
- If monitoring indicates that accepted procedures are not taking place, **corrective action** should be put in place **using the procedures in a RACA's own quality assurance processes.**
- If accepted procedures are not being adhered to, **remove the known customer from the Register and inform CAA.** CAA will then inform the wider industry.

Appendix F – Transhipment Cargo