Australian Government
Civil Aviation Safety Authority

ADVISORY CIRCULAR
AC 11-03 v3.0

Electronically formatted certifications, records and management systems

Date July 2022

File ref D22/248358

Advisory circulars are intended to provide advice and guidance to illustrate a means, but not necessarily the only means, of complying with the Regulations, or to explain certain regulatory requirements by providing informative, interpretative and explanatory material.

Advisory circulars should always be read in conjunction with the relevant regulations.

Audience

This Advisory Circular (AC) has general application to anyone seeking to meet the legislative requirements set under the Civil Aviation Act 1988 (CAA), Civil Aviation Safety Regulations 1998 (CASR), Civil Aviation Regulations 1988 (CAR), or any Manuals of Standards (MOS) or Civil Aviation Orders (CAO); especially those involved in designing, certifying, operating or maintaining aircraft.

The information and concepts described within this AC are intended to address both a web based (online) and stand-alone system.

Purpose

This AC provides guidance on the use of electronically formatted certifications (signatures), records, organisation manuals and electronic management systems to satisfy regulatory requirements under the CAA, CASR, CAR, MOS and the CAOs. This AC also provides guidance on the CASA approval of electronic systems.

The document expresses CASA's policy on the acceptance of the electronic equivalent of many matters historically accomplished using paper format.

For further information

For further information, contact CASA's Advisory and Drafting Branch (telephone 131 757).

Unless specified otherwise, all subregulations, regulations, Divisions, Subparts and Parts referenced in this AC are references to the *Civil Aviation Safety Regulations 1998 (CASR)*.

Status

This version of the AC is approved by the Branch Manager, Advisory and Drafting, Legal, International and Regulatory Affairs.

Note: Changes made in the current version are not annotated. The document should be read in full.

Version	Date	Details
v3.0	July 2022	This revision updates the format of the AC and includes advice relating to electronic document rules incorporated into Parts 91, 121, 133, 135 and 138 of CASR on 2 December 2021.
(1)	May 2013	This is the second version of this Advisory Circular (AC). This AC has been adjusted to accord with the Electronic Transactions Amendment Act 2011 (Cth) which amended section 10 of the ETA. Amendments to the AC have been marked with shading. As a result of the 2011 amendment, an electronic signature must be capable of indicating the signatory's 'intention' in respect of the information contained in the electronic communication, rather than the signatory's 'approval' of the information contained in the electronic communication. Prior to the 2011 amendment, the requirement of section 10(1)(b) of the ETA was that "having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated." The amending Act repeals paragraph 10(1)(b) of the ETA and substitutes a new paragraph to this 'reliability test' for determining whether the method used was as 'reliable as was appropriate' by adding reference to 'in light of all of the circumstances including any relevant agreement'. The amendment also validates a signature method regardless of its reliability in principle, in circumstances where the method used is proven in fact to have identified the signatory, and indicated the signatory's intention in respect of the information contained in the electronic communication, by itself or together with further evidence.
(0)	November 2012	This is the first Advisory Circular (AC) to be written on the subject.

Contents

1 Reference material

1.1 Acronyms

The acronyms and abbreviations used in this AC are listed in the table below.

Acronym	Description
AC	advisory circular
AOC	Air Operator's Certificate
AMO	Approved Maintenance Organisation
ARN	Aviation Reference Number
CAA	*Civil Aviation Act 1988*
CAR	*Civil Aviation Regulations 1988*
CASA	Civil Aviation Safety Authority
CASR	*Civil Aviation Safety Regulations 1998*
CRS	Certificate of Release to Service
ETA	*Electronic Transactions Act 1999*
LAME	Licensed Aircraft Maintenance Engineer
MEL	minimum equipment list
MOS	Manual of Standards
NAA	National Aviation Authority

1.2 Definitions

Terms that have specific meaning within this AC are defined in the table below. Where definitions from the civil aviation legislation have been reproduced for ease of reference, these are identified by 'grey shading'. Should there be a discrepancy between a definition given in this AC and the civil aviation legislation, the definition in the legislation prevails.

Term	Definition
Authentication	Means by which a system validates the identity of an authorised user. This may include a password, a personal identification number (PIN), a cryptographic key, a badge, or a stamp. Authenticate means to validate or establish to be genuine such that the matter being authenticated will have legal force or be legally binding.
Electronic Signature	Any signature made using an electronic communication. Where an electronic signature is used to satisfy a requirement under Commonwealth law, a method should be used that identifies the person and indicates the person's intention in respect of the information communicated. Also, the method used needs to be as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or proven in fact to have identified the signatory, and indicated the signatory's intention in respect of the information contained in the electronic communication, by itself or

Term	Definition
	together with further evidence. The method used needs to comply with the relevant Government agency's requirements for applying that method. An electronic signature can combine cryptographic functions of digital signatures with the image of a person's handwritten signature or some other form of visible mark that would be considered acceptable in the circumstances.
Signature	Any method used to identify a person and to indicate the signatory's intention in respect of the information contained in the communication (e.g., the execution of a particular document may need to be witnessed, and in these circumstances, the witness' signature merely identifies the signatory as a witness to the execution of the document), or the signatory's approval of the information communicated (e.g. to attest to the completion of, or a person's involvement in, an act, or to certify a record entry). Signatures can be handwritten or electronic.

1.3 References

Legislation

Legislation is available on the Federal Register of Legislation website https://www.legislation.gov.au/

Document	Title
	Civil Aviation Act 1988
	Electronic Transaction Act 1999
	Electronic Transaction Amendment Act 2011
	Electronic Transactions Regulations 2000
Part 11 of CASR	Regulatory administrative procedures
Regulation 91.100 of CASR	Electronic documents
Regulation 121.075 of CASR	Electronic documents
Regulation 131.265 of CASR	Electronic documents
Regulation 133.045 of CASR	Electronic documents
Regulation 135.055 of CASR	Electronic documents
Regulation 138.220 of CASR	Electronic documents

Advisory material

CASA's advisory materials are available at https://www.casa.gov.au/publications-and-resources/guidance-materials

Document	Title
AC 91-07	Cabin electronic flight bags
AC 91-17	Electronic flight bags
Part 91 AMC/GM	Acceptable means of compliance / guidance material - General operating and flight rules
Part 121 AMC/GM	Acceptable means of compliance / guidance material - Australian air transport operations - larger aeroplanes
Part 131 AMC/GM	Acceptable means of compliance / guidance material - Balloons and hot air airships
Part 133 AMC/GM	Acceptable means of compliance / guidance material - Australian air transport operations - rotorcraft
Part 135 AMC/GM	Acceptable means of compliance / guidance material - Australian air transport operations - smaller aeroplanes
Part 138 AMC/GM	Acceptable means of compliance / guidance material - Aerial work operations

2 Background

2.1.1 As the complexity of aircraft design, certification, operations and maintenance processes increased, the number of records and documents generated and required to be retained by aircraft registered operators, manufacturers and approved maintenance organisations expanded significantly. The development of electronic information storage and retrieval systems has significantly enhanced the ability of the aviation industry not only to meet regulatory record-retention requirements; but also to manufacture, operate, and maintain today's highly complex aircraft and aircraft systems in a demanding operational environment.

2.1.2 It is widespread for the general community and the aviation sector, to utilise electronic certifications and signatures, logbooks [chronological compliance records] and programs/controls (e.g. computer software programs or tablet / phone apps) containing navigation charts and weight and balance calculators.

2.1.3 Before electronic signatures were commonly recognised, a handwritten signature was the primary means by which an individual could comply with the requirement for a signature on any required record, record entry, or document. Although an electronic signature may be essentially a new form of signature, its purpose is identical to that of a handwritten signature.

2.1.4 Although the use of electronic signatures enhances the ability to identify a signatory and helps to eliminate the traceability difficulties associated with illegible handwritten entries and the deterioration of paper documentation, they must possess certain qualities and attributes to be acceptable. These qualities and attributes are specified at paragraph 3.2.4.

3 Relevant legislative provisions

3.1.1 The key legislative provisions relating to electronically formatted certifications, records and management systems are contained in the ETA 1999, Part 11 of CASR and regulations 91.100, 121.075, 131.265, 133.045, 135.055 and 138.220 of CASR.

3.2 Electronic Transactions Act

3.2.1 The ETA provides that a Commonwealth law requiring or permitting written information, a signature, or the retention of information, can be satisfied electronically (unless specifically excluded by another Commonwealth law). It allows people to communicate electronically with Government agencies and to use electronic communications/record systems to satisfy their legal obligations.

3.2.2 Section 8 of the ETA 1999 establishes a general rule that for the purpose of a law of the Commonwealth, a transaction is not invalid because it takes place wholly or partly by means of one or more electronic communications. The ETA provides that the following requirements under a law of the Commonwealth can be met in electronic form:

- a requirement to give information in writing (section 9 of the ETA 1999)
- a requirement to provide a signature (section 10 of the ETA 1999)
- a requirement to produce a document (section 11 of the ETA 1999)
- a requirement to record and retain information (section 12 of the ETA 1999).

3.2.3 These provisions are subject to certain criteria being met. In relation to electronic communications that are required or permitted to be given to Government agencies, the following criteria apply:

- **Readily accessible condition:** It must be reasonable to expect that, at the time information in the communication is given, recorded or generated, the information would be readily accessible so as to be useable for subsequent reference.
- **Integrity:** The information contained in the communication must retain its integrity. This means the information must remain complete and unaltered (apart from the addition of an endorsement, or any immaterial change arising in the normal course of communication, storage or display). This may include, for example, information added to the communication that is necessary to identify the message for storage purposes.
- **Specified information technology requirements:** Where an agency specifies particular information technology requirements for accepting the communication (e.g. that it must be provided in a particular format) those requirements must be met.
- **Specified verification procedure:** Where an agency specifies a procedure for verifying the receipt of the communication, the person providing the communication must comply with and complete that procedure.

3.2.4 In relation to a requirement to provide a signature under a Commonwealth law, section 10 of the ETA 1999 specifies that the following elements that must be satisfied if an electronic signature method is used:

- the method identifies the person and indicates the person’s intention in respect of the information communicated; and

- the method used was either:
  - as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
  - proven in fact to have fulfilled the functions described in paragraph a), by itself or together with further evidence.

3.2.5 The final required circumstance is, in the case of a signature required to be given to a Commonwealth entity, that the method must comply with any particular information technology specifications of that entity and, in the case of any other party, that it has consented to the use of the method (ETA paragraphs 10(1)(c) and (d)).

3.2.6 Section 10 of the ETA does not affect the operation of any other law of the Commonwealth that makes provision for, or in relation to, requiring:

- an electronic communication to contain an electronic signature (however described)
- an electronic communication to contain a unique identification in an electronic form
- a particular method to be used in relation to an electronic communication to identify the originator of the communication and to indicate the originator's intention in respect of the information communicated.

3.2.7 The following factors may be taken into account when determining the appropriateness of the signature method adopted:

- the function of the signature requirements in the relevant statutory environment
- the type of transaction
- the capability and sophistication of the relevant communication systems
- the value and importance of the information in the electronic communication.

3.3 Civil Aviation Safety Regulations 1998

3.3.1 The CASR authorises CASA to specify particular forms for authorisation applications and other documents. Regulation 11.015 of the CASR 1998 defines 'authorisation' as any of the following:

- a civil aviation authorisation (as defined in section 3 of the CAA 1988) other than an AOC, a delegation or an appointment of an authorised person
- an approval or qualification of a document or thing under the CASR or the CAR (other than a material, part, process or appliance to which Subpart 21.K of the CASR 1998 applies)
- a certificate capable of being granted to a person under the CASR or the CAR.

3.3.2 Subregulation 11.030 (1) of the CASR provides that an application for an authorisation is not taken to have been made unless:

- it is made in the manner approved by CASA for that purpose
- if CASA has approved a form for the application — it is in the approved form and includes all of the information required by the form
- it includes all the information required by the CASR or the CAR
- it is accompanied by every document required by the CASR or the CAR
- if a fee is payable for the application — that fee has been paid.

3.3.3 Regulation 11.018 of the CASR provides that if CASA has approved a form for a document, other than an application for authorisation, the document is not taken to have been completed unless it:

- is in the approved form
- includes all of the information required by the form.

3.3.4 Guidance material relating to specific electronic document regulations and requirements contained within Parts 91, 121, 131, 133, 135 and 138 of CASR is available and published by CASA. Refer to the list of advisory material in the Reference material section at the beginning of this AC.

3.4 Civil Aviation Act 1988

3.4.1 The CAA also contains provisions authorising CASA to specify particular forms for civil aviation authorisations. For example, section 27AA of the CAA 1988 states that an application for an AOC must be in a form approved by CASA.

3.5 Application of legislative provisions to CASA

3.5.1 The ETA sets a framework for Government agencies to manage their information resources in a manner that will allow for greater electronic engagement with stakeholders, improve the utility of information for users and enhance the capacity for information to be stored electronically. It means that people engaging with CASA in relation to its statutory functions can generally conduct transactions (e.g. making applications, lodging returns or certificates, or giving information) electronically.

3.5.2 The aviation regulations have not specifically restricted the use of electronic information management systems or the use of electronic signatures. Nor do the regulations specify that forms required by CASA in relation to its civil aviation functions must be in a particular format. Historically, they did anticipate a paper-based outcome which resulted in paper-based systems being preferred to electronic ones.

3.5.3 However, the legislative provisions discussed above do provide that CASA may do any of the following:

- approve a form for an AOC application under section 27AA of the CAA in either an electronic or paper format
- require a person giving information to do so by means of a particular kind of electronic communication and according to particular information technology requirements
- require a person giving information to take a particular action to verify the receipt of the information
- specify that it will receive information on particular forms made available on its website or elsewhere.

4 Common matters for electronically formatted certification, record or management systems

4.1 General outcomes

4.1.1 Where an aviation regulation specifies a requirement to do any of the things below, that requirement can be met in electronic form subject to the requirements outlined in paragraph 5.1.2:

- give information in writing
- provide a signature
- produce a document
- record information
- retain a document.

4.1.2 The attributes of the electronic systems used to meet those requirements must be able to deliver the following outcomes:

- The electronic display of a record that is a log (chronological record history) can provide the display in chronological order.
- The person responsible for the retention of records can inform CASA of a person who has custody of the record and who is able to produce that record.
- If the custody of an aircraft or operational record has been transferred from another person (e.g. when an aircraft is imported into Australia) the transferred records are retained as part of the record that can be produced if required.
- The requirement to produce a document is not nullified by the destruction of a primary data storage. The electronic system needs to be capable of reconstructing the record if there is a requirement to retain a signature, document or information.
- There is a reliable means of assuring the maintenance of the integrity of the information:
  - This could be accomplished by having a record of transactions including records of entries and alterations of entries which identifies the person by name, date and ARN who makes the entry and any alteration.
  - Corrected errors are alterations to the record that need to be identified as and include the reason for the correction.
- The system design takes account of the effort involved in recording information (e.g., the ease of carriage for the electronic recording, certification or management device and the accuracy/continuity of the recorded information).
- There is a mechanism for version control to ensure that, where a document is changed, those changes can be tracked and all users can access the current version.

4.1.3 Irrespective of how a required document is generated, or what format it takes, the applicant must be able to demonstrate that all the necessary legislative requirements from the CAA, CASR, CAR and associated MOS/CAO are met.

4.1.4 Where employees require access to online documents, this must be considered in the system design. Access would need to be such that the system is sufficiently stable and

incorporates any backup mechanisms required to allow the organisation to meet access requirements in the case of any system failure.

4.2 Security

4.2.1 It is strongly recommended that an electronically formatted certification, record or management system include security mechanisms with the following attributes:

- The electronic system maintains information confidentially.
- The system ensures that there cannot be unauthorised alterations to the record.
- The system is supported by a policy and management structure that supports the hardware and software which delivers the information.

4.2.2 It is strongly recommended that an organisation's exposition/procedures include the following matters to enable the exposition and/or procedures to be determined to be adequate for their purpose:

- a mechanism for version control
- an audit procedure that can ensure the integrity of each computerised workstation and verify whether records have been accessed improperly
- a procedure for conducting a review of the use of any personal identification codes by the system to ensure that it will not permit password duplication
- a procedure which establishes an audit of the computer system at a frequency sufficient to ensure the integrity of the system (e.g., by demonstrating that access to records is restricted to authorised persons or applications)
- a procedure which describes how it will ensure that the computerised records will be transmitted to other organisations in a format acceptable to them
- a procedure for making required records available to CASA personnel (e.g., by providing access to the system via a logon portal) so that they can make paper copies of viewed information
- guidelines for the use of electronic signatures for contractors
- a description of the training procedure and requirements to authorise access to the system.

5 Electronic record keeping systems

5.1.1 As described below, there is considerable variety in the way organisations utilise electronic recordkeeping systems including the degree to which they use them. The following examples reflect the various levels of technology that may be used and outline how each system can meet the requirements of a certification/record keeping system.

5.1.2 **Paper records** – Such a system is based on an electronically generated records consisting of work packages printed on paper. The paper record controls the activities to be performed and any required certification is recorded by hand. The paper data record is then entered into the electronic data base. This level of electronic recording does not have a separate log of certifications so the paper records containing the certifications would need to be retained. If the paper records are scanned for retention in a database then the paper record of certifications would not need to be retained.

5.1.3 **Paperless** – Single Function System. Such a system is paperless and meets the requirements for an electronic controlled system of certification. The maintenance requirements may be electronically generated from a database or manually input from a paper document. Worksheets will be electronically generated viewed on a monitor or display and records are stored electronically.

For an AMO example:

A maintenance certification for the conduct of the maintenance task is electronically recorded by the person performing the maintenance and an electronic CRS for all of the maintenance tasks on the aircraft is signed at completion.

The record is then electronically closed and filed; however, if the work task is part of a comprehensive maintenance package the system architecture may allow for that record to remain open until the completion of the maintenance package is coordinated.

5.1.4 **Paperless** – Integrated Functions. Such a system is a true paperless system that covers a fully integrated package and are typically used by larger organisations.

An airline example of the integration could include:

- Flight Operations – electronic flight plans, electronically ordering fuel, electronic weather reports, etc.
- Flight Services – electronic passenger list, catering and in-flight services ordered and confirmed electronically.
- Maintenance – maintenance planning, maintenance watch control, stores/supply (e.g. component tracking by bar code) line and heavy maintenance terminals.
- Load control – electronic transmission to aircraft loaders and trim sheet to flight crew and dispatch.
- Ramp Services – aircraft servicing requirements, electronic notification of fuel loaded to flight crew and load control.
- Flight Crew – (in cockpit) electronic notification of aircraft readiness, load sheet, fuel docket, final flight plan, passenger loading complete. Release by maintenance including MELs and deferred defects.
- Personnel – Record - training and currency.

6 Electronic certifications/signatures

6.1 Recommended practice

6.1.1 An electronic record keeping system that includes electronic signatures will be reviewed by CASA during entry control when organisational processes are assessed for suitability.

6.1.2 Some of the considerations relating to electronic signatures that must be assessed are:

- Relevant records are available to CASA in a readily accessible condition for monitoring and review purposes and are capable of displaying the following:
  - personnel identity (e.g., LAME) – signature and ARN issued by CASA; and
  - organisational identity (e.g.) AMO – signature and identification issued by AMO.

Note: A signature comprising merely a person's name and initials may sometimes be acceptable for these purposes.

- All electronic records must be available in a readily accessible condition so that they:
  - are readable in plain language on the display unit; and
  - can be printed in hard copy where required.
- To guarantee the authenticity of records, the system must be capable of:
  - establishing if the records have been altered by any person or process;
  - establishing the reliability of software applications used to create records;
  - displaying the time and date records were created or altered;
  - demonstrating the name and identity of any person who created, accessed or altered them; and
  - displaying an altered record prior to and after its alteration.

6.1.3 The prior acceptance, by an aircraft designer/manufacturer, of a system of electronic recordkeeping system or a system using electronic signatures does not mean an automatic acceptance by CASA for use of the product by your organisation. While the software and hardware may be the same, CASA's assessment is based on how you will use the system (as described in your exposition/procedures manual) and what you propose to do with that system.

6.2 Recommended practice

6.2.1 An electronic signature should not be capable of being affixed to a record where the person's qualification and authorisation are not appropriate to the record.

6.2.2 Examples of the way in which such a system would work include:

- a B2 Avionic LAME prevented from affixing their electronic signature to a B1 mechanical specific task
- where the employee's recurrent/continuation training or skill level requirements are not appropriate to the task being carried out the system provides a warning or prevents an entry

- where two separate signatures are required (e.g., an independent inspection for a flight critical task), the system requires both signatures and identification for the record to be complete.

6.3 Forms of electronic signatures

6.3.1 An electronic signature may be in the form of a digital signature, a digitised image of a paper signature, a typed notation, an electronic code, or any other acceptable form of individual identification that can be reliably used to attest a record, record entry, or document.

6.3.2 Not all identifying information found in an electronic system may constitute a signature. For example, the entry of an individual's name in an electronic system may not constitute an electronic signature.

6.4 The functions and characteristics of a signature

6.4.1 A signature is capable of performing a number of functions, namely it can:

- identify the signatory
- provide certainty as to the personal involvement of a particular person in the act of signing
- associate a particular person with the contents of the document
- attest to the intention of a person to be bound by the contents of the document
- attest to authorship of the document by the signatory
- attest to some written agreement which may have been written by some third party who is not a party to the binding agreement.

6.4.2 Before CASA can accept an electronic signature for certification purposes, the method used must be able to reliably identify the signatory in a way that is difficult for an unauthorised person to duplicate. This can be done by using an authentication procedure that validates the identity of the signatory. The signature must also include the licence or certificate number issued by CASA or, where the person is exercising an authorisation issued by an organisation, that identification.

6.4.3 For example, an individual using an electronic signature should be required to identify themselves and the system that produces the electronic signature should then authenticate that identification.

6.4.4 A computer entry used as a signature should have restricted access that is limited by an authentication code that is changed periodically. Access to issued stamps or authentication codes should be limited to the user. Although a signature may take many forms, CASA emphasises that all electronic entries may not necessarily satisfy the criteria that would qualify an electronic entry as an acceptable signature.

6.4.5 Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes. These codes could be encoded onto badges, cards, cryptographic keys, or other objects. Systems using PINs or passwords memorised by an individual could also serve as an acceptable method of ensuring uniqueness. Additionally, a system could also use physical characteristics, such as a

fingerprint, handprint, or voice pattern, etc as a method of identification and authorisation.

6.4.6 **Significance**. An individual using an electronic signature should take deliberate and recognisable action to affix his or her signature (e.g. using badge swipes, signing an electronic document with a stylus, inputting a specific keystroke(s), or using a digital signature).

6.4.7 **Scope**. The scope of information attested by an electronic signature must be understood by the signatory and be apparent to subsequent readers of the record, record entry, or document. While handwritten documents use the physical proximity of the signature to the information in order to identify those items attested to by a signature, electronic documents may not use the position of a signature in the same way. It is therefore important to clearly delineate the specific sections of a record or document that are affected by a signature from those sections that are not affected. Acceptable methods of delineation of the affected areas include, but are not limited to: highlighting, contrast inversion or the use of borders or flashing characters. In addition, the system should notify the signatory that the signature has been affixed.

6.4.8 **Signature Security**. The security of an individual's handwritten signature is maintained by ensuring it is difficult for another person to duplicate or alter it. An electronic signature should maintain an equivalent level of security. Due to the reproduction capability inherent in an electronic system, an electronic system used to produce a signature should restrict the ability of any person to cause another individual's signature to be affixed to record, record entry, or document. Such a system enhances safety by precluding an unauthorised person from certifying required documents, such as a maintenance release. The signatory must also know who else holds the privilege for access to the electronic authentication key.

6.4.9 **Non-repudiation**. An electronic signature should prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document. The more difficult it is to duplicate a signature, the greater the likelihood that a signature was created by the signatory. Those security features of an electronic system that make it difficult for another person to duplicate a signature or alter a signed document tend to ensure that a signature was indeed made by the signatory.

6.4.10 **Traceability**. An electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document.

7 Electronic management systems

7.1.1 There is a wide range of commonly available electronic devices and programs which assist with the conduct and management of aircraft related activities. The level of CASA's review of operator procedures and devices used as an electronic management system for these purposes will depend on where the systems will be used and what the programs will be used to accomplish. Devices used in aircraft may require airworthiness approval.

7.1.2 For further information regarding the use of electronic flight bags, refer to AC 91-17. For information regarding the use of cabin electronic flight bags, refer to AC 91-07.

7.1.3 Matters to be considered for an electronic management system include:

- confirmation that the calculations used in the program are correct
- connectivity – wireless systems
- power connections
- software applications
- hardware
- mounts
- cabling
- stowage
- security
- electromagnetic interference
- electromagnetic compatibility
- procedures and updates.