RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington D.C. 20036

Aeronautical Information System Security Glossary

RTCA Paper No. 120-21/PMC-2151
June 17, 2021

Prepared by: SC-216

Copies of this document may be obtained from

RTCA, Inc.
1150 18th Street, N.W., Suite 910
Washington, DC 20036

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please call RTCA for ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) and EUROCAE Working Group 72 (WG-72). It was approved for release March 19, 2021.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;
- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency;
- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and
- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunications Union and other appropriate international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate**.**

This Page Intentionally Left Blank

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This document is concerned with providing a glossary of terms for Aeronautical Information Systems Security (AISS). This Glossary is primarily intended to provide assistance to the users of the following EUROCAE and RTCA Documents:

ED-201	*Aeronautical Information System Security (AISS) Framework Guidance* (2015)
ED-202A/DO-326A	*Airworthiness Security Process Specification* (2014)
ED-203A/DO-356A	*Airworthiness Security Methods and Considerations* (2015)
ED-204/DO-355	*Information Security Guidance for Continuing Airworthiness* (2014)
ED-204A/DO-355A	*Information Security Guidance for Continuing Airworthiness* (2020)
ED-205	*Process Specification for security Certification of Air Traffic Management/Air Navigation Services (ATM/ANS) Ground Systems* (2019)

The definitions represent the meanings understood and shared by the Aeronautical Information System Security Community and each Term in the Glossary definitions has a cross reference to the information source.

This Page Intentionally Left Blank

CHAPTER 2

DEFINITIONS AND REFERENCES

This chapter provides for the Definitions of Terms in TABLE 1 and for References to non-EUROCAE/non-RTCA documents, from which definitions have been adopted.

TABLE 1: DEFINITION OF TERMS

Term	Definition	Source
Access Control	Security service that controls the use of resources and the disclosure and modification of data.	NIAP CIM-BRE
Accountability	Property that allows activities in an IT system to be traced to the entity responsible for the activity.	NIAP CIM-BRE
Activity	Tasks that provide a means of meeting the objectives.	ED-204A/DO-355A
Aeronautical Information System	The set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information involved in all aspects of aircraft operations. Note that this includes supplier's information systems supporting the development of onboard system software and data.	ED-202A/DO-326A adapted from: Title 44 U.S.C., §3502 (8)
Airborne Software	Airborne Software includes all programs and data that are included in an aircraft system safety assessment or requires flight operations approval or requires maintenance operations approval. Airborne software encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)) and Hardware Controlled Software (HCS) as defined in ARINC 667-1 [Source: ARINC 667].	ARINC 667-1 ED-203A/DO-326A
	Airborne software encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)), Hardware Controlled Software (HCS) and Firmware (configuration of FPGAs (Field Programmable Gate Arrays) and other complex electronic hardware).	ED-204A/DO-355A
Aircraft	An aircraft or "aeroplane" means an engine-driven fixed-wing aircraft heavier than air that is supported in flight by the dynamic reaction of the air against its wings" (from Regulation (EU) No 965/2012).	ED-204A/DO-355A
	Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface.	ICAO Doc 9713, 2nd Ed., 2001

Term	Definition	Source
Aircraft Component	Any self-contained part, combination of parts, subassemblies or units, that perform a distinctive function necessary to the operation of the system.	SAE ARP 4754A, "Component"
	An aircraft component is a component approved for installation on a type-certified aircraft.	ED-204A/DO-355A
Aircraft Domain	see Domain (Aircraft).	
Aircraft Information Security Center	The Aircraft Information Security Center should act as the operator's point of contact for aircraft information security events from within and outside the operator's organization.	ED-204A/DO-355A
Aircraft Type Certification	Design approval of an aircraft establishing that it ensures compliance with the applicable airworthiness requirements.	ED-204A/DO-355A
Air Gap	*An interface between two systems at which they are not connected physically*, electrically or electro-magnetically (incl. optically).	inspired by IETF RFC 4949
Air Traffic Management (ATM)	The dynamic, integrated management of air traffic and airspace including air traffic services, airspace management and air traffic flow management — safely, economically and efficiently — through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based functions.	ICAO Doc 4444 15th Ed., 2007
Airworthiness	The condition of an aircraft, aircraft system, or component in which it operates in a safe manner to accomplish its intended function.	SAE ARP 4754A
Airworthiness Security (AWS)	The protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data and/or data interfaces. This also includes the consequences of malware and forged data and of access of other systems to aircraft systems.	ED-202A/DO-326A ED-204A/DO-355A
	The protection of the airworthiness of an aircraft from "intentional unauthorized electronic interaction.	ED-203A/DO-356A
Anonymity	The condition of an identity being unknown or concealed.	IETF RFC 4949

Term	Definition	Source
Anonymous	An application may require security services that maintain anonymity of users or other system entities, perhaps to preserve their privacy or hide them from attack. To hide an entity's real name, an alias may be used. For example, a financial institution may assign an account number. Parties to a transaction can thus remain relatively anonymous, but can also accept the transaction as legitimate. Real names of the parties cannot be easily determined by observers of the transaction, but an authorized third party may be able to map an alias to a real name, such as by presenting the institution with a court order. In other applications, anonymous entities may be completely untraceable.	IETF RFC 2828
Appropriate authority	The entity to which Declaration is made or who certifies the system.	ED-205
Assessment	An evaluation based upon engineering judgment.	SAE ARP 4754A
Asset(s)	The logical and physical resources of the aircraft which contribute to the airworthiness of the aircraft, including functions, systems, items, data, interfaces, processes and information.	ED-202A/DO-326A
	What has value to the organization and which therefore requires protection. Note: Assets can have (for example) a financial, operational or intellectual property value.	ISO/IEC 27005:2011
Assumptions	Statements, principles, and/or premises offered without proof.	SAE ARP 4754A
Assurance	The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements.	ED-12B/DO-178B, ED-12C/DO-178C
Assurance (Information)	See Information Assurance.	
Attack	An assault on a system that derives from an act that is an attempt to violate the security policy of a system. This includes intentional and unintentional acts.	ED-202A/DO-326A DO-204A/DO-355A Adapted from IETF RFC 2828 "attack"
	An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.	IETF RFC 2828
Attack Path	The path, interface, and actions by which an attacker executes an attack.	ED-202A/DO-326A

Term	Definition	Source
Attack Vector	The means of access which an attacker used to begin an attack.	ED-202A/DO-326A
Attacker	The entity that initiates and directs an attack. This includes intelligent attacker as well the automatic actions of attack code such as a bot or worm, as well as the authors of such code.	ED-202A/DO-326A
Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. **NOTE 1 TO ENTRY:** An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). **NOTE 3 TO ENTRY:** "Audit evidence" and "audit criteria" are defined in ISO 19011.	ED-205 ISO/IEC 27000:2016
Audit (Security)	See Security Audit.	
Audit Trail (Security)	See Security Audit Trail.	
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.	NIST SP800-53, Rev 5
Availability	**Security usage:** Ensuring authorized users have access to information and associated assets when required	ED-203A/ED-205 ISO17799 (Withdrawn)
	Safety Usage: Qualitative or quantitative attribute that a system or item is in a functioning state at a given point in time. It is sometimes expressed in terms of the probability of the system (item) not providing its output(s) (i.e. unavailability).	SAE ARP 4754A
Biometrics	An automatic identification process for identity verification of individuals based on unique behavioral or physiological characteristics. These are unique things that we do or unique physical characteristics that we have. Behavioral biometrics include voice, signature, and keyboard typing technique. Physical biometrics include fingerprint, hand geometry, facial recognition, and iris and retinal scan.	GSA GSCH, 2004
Certificate (Digital)	See Digital Certificate.	

Term	Definition	Source
Certificate (Public Key)	See Digital Certificate.	
Certificate Authority (CA)	A component of the Public Key Infrastructure. The CA is responsible for issuing and verifying digital certificates.	GSA GSCH, 2004
	Synonym for "certification authority". Deprecated Term: IDOCs SHOULD NOT use this term; it suggests careless use of the term "certification authority", which is preferred in PKI standards (e.g., [X509, R3280])	IETF RFC 4949
Certificate Revocation List (CRL)	A computer file that contains the list of all digital certificates that is revoked and thus is no longer valid and reliable.	ED-204A/DO-355A
	A periodically issued list, digitally signed by a CA, of identified certificates that have been suspended or revoked prior to their expiration dates.	GSA GSCH, 2004
	A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, delta CRL, X.509 certificate revocation list.)	IETF RFC 4949
Certification	**Aeronautical usage**: see Aircraft Type Certification	SAE ARP 4754A
	Any form of recognition based on an appropriate assessment, that a legal or natural person, ATM/ANS system, ATM/ANS constituent complies with the applicable requirements, through the issuance of a certificate attesting such compliance	ED-205
	Information system usage: Comprehensive evaluation (usually made in support of an accreditation action) of an information system's technical security features and other safeguards to establish the extent to which the system's design and implementation meet specified security requirements.	IETF RFC 4949
Claims	"Claim" is a shorthand notation for a "Security Conformance Claim". It includes an identification of security requirements for which the conformance is claimed. It has a statement about the conformance or conditions influencing the claim. A rationale is provided that assists the evaluator in confirming if the claim is acceptable by checking whether it meets all requirements for content and presentation of evidence.	ED-205
Common Criteria	"The Common Criteria" is a standard for evaluating information technology products and systems, such as operating systems, computer networks, distributed systems, and applications. It states requirements for security functions and for assurance measures.	IETF RFC 2828

Term	Definition	Source
	A standard for evaluating information technology (IT) products and systems. It states requirements for security functions and for assurance measures.	IETF RFC 4949
	The CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation.	Common Criteria, Part 1, version 3.1, Rev 4
Completeness	Completeness is the degree to which a set of correct requirements, when met by a system, satisfy the interests of customers, users, maintainers, certification authorities as well as aircraft, system and item developers under all modes of operation and lifecycle phases for the defined operating environment.	ED-79A / ARP4754A No definition, paragraph extract Section 5.4.2(c)
Component	Any self-contained part, combination of parts, subassemblies or units, that perform a distinctive function necessary to the operation of the system.	ED-79A / ARP4754A
Compromise	**Data usage**: A security incident in which information is exposed to potential unauthorized access, such that unauthorized disclosure, alteration, or use of the information might have occurred.	IETF RFC 2828 IETF RFC 4949
	Security usage: A security violation in which a system resource is exposed, or is potentially exposed, to unauthorized access.	IETF RFC 2828 IETF RFC 4949
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO 27000:2018 ED-203A/DO-356A/ ED-205 refers to previous ISO 27000 2016 same definition
Consequence	Outcome of an event affecting objectives. ***NOTE 1 TO ENTRY:*** *An event can lead to a range of consequences.* ***NOTE 2 TO ENTRY:*** *A consequence can be certain or uncertain and, in the context of information security, is usually negative.* ***NOTE 3 TO ENTRY:*** *Consequences can be expressed qualitatively or quantitatively.* ***NOTE 4 TO ENTRY:*** *Initial consequences can escalate through knock-on effects.*	ISO/IEC 27000:2018 ED-205 refers to ISO 27000 2016 same definition

Term	Definition	Source
Consistent	Consistency between requirements statements means the attributes are in agreement within the scope of the intended purposes. A design specification is consistent with the requirements if neither contradicts the other. A power budget summary is consistent with a design specification if a quantity in the budget that refers to the design specification is equal to the quantity implied by the design specification.	ED-202A/DO-326A
Continued Airworthiness	All the actions associated with the upkeep of a type design and the associated approved data through life.	ED-204A/DO-355A
Continuing Airworthiness	All of the processes ensuring that, at any time in its operating life, the aircraft complies with the airworthiness requirements in force and is in a condition for safe operation.	ED-204A/DO-355A
Control (Security)	See Security Control.	
Correctness	The degree to which an individual requirement is unambiguous, verifiable, consistent with other requirements and necessary for the requirement set.	ED-79A / ARP4754A No definition, paragraph extract Section 5.4.2(c)
Crate	Digital container for aircraft software parts and related digital products used for electronic distribution between aerospace business partners.	ARINC 827
Cryptographic Key (Key)	Usually shortened to just “key”. An input parameter that varies the transformation performed by a cryptographic algorithm.	IETF RFC 2828, IETF RFC 4949

Term	Definition	Source
Design Approval Holder (DAH)	A design approval holder is the holder of a type certificate, a Parts Manufacturer Approval or a Technical Standard Order authorization or the licensee of a Type Certificate. ***NOTE:*** *References to a type certificate includes supplemental type certificates unless noted otherwise.* All design approval holders must: • Report failures, malfunctions, and defects • Make Instruction for Continued Airworthiness (including changes) available to each aircraft, aircraft engine or propeller owner • Satisfy Additional Obligations for: Parts Manufacturer Approval Holder, Technical Standard Order Authorization Holders and Type Certificate Holders [Source: FAA]	ED-204A/DO-355A
Data	Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world.	Hansen, 1973
Data distribution	The ground based process of moving airborne software and data from a source location to a destination location and the process of storing software and data at each location. Examples of source and destination locations are software vaults, airborne software servers, Aircraft on-board mass storage, and OEM software distribution systems.	ED-204A/DO-355A
Data Loading	The process of moving airborne software and data from a storage source into the active executable memory of aircraft systems. Examples of storage sources are aircraft on-board mass storage, Portable Data Loader (PDL) mass storage or media, Aircraft Data Loader (ADL) mass storage or media, and software vault servers.	ED-204A/DO-355A
Declaration	Declaration' means any written statement made under the sole responsibility of a legal or natural person to confirm that the applicable requirements relating to a legal or natural person, ATM/ANS system, or ATM/ANS constituent are complied with.	ED-205
Defense in Depth	An architectural strategy in which more than one security measure is used such that a successful attack would require vulnerabilities in multiple security measures.	ED-204A/DO-355A
Dependent System	An aircraft system that depends on an external system for correct function.	ED-202A/DO-326A
Development Error	A mistake in requirements determination, design or implementation.	ED-79A / ARP4754A

Term	Definition	Source
Digital Certificate	A digital representation of information which at least (a) identifies the certification authority issuing it, (b) names or identifies its subscriber, (c) contains the subscriber's public key, (d) identifies its operational period, and (e) is digitally signed by the certification authority issuing it. [Ed see also Public Key Certificate].	NIST SP800-32: "Certificate"
	The term digital certificate refers to the private key and the associated public key of the digital certificate. The sender's private key is used for signing and the receiver's private key for decrypting; the sender's public key is used to verify the signature and receiver's public key for encrypting.	ED-204A/DO-355A
	A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object.	IETF RFC 4949
Digital Signature	A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.	IETF RFC 2828, IETF RFC 4949
Discretionary Access Control (DAC)	An access control service that enforces a security policy based on the identity of system entities and their authorizations to access system resources.	IETF RFC 2828
	An access control service that (a) enforces a security policy based on the identity of system entities and the authorizations associated with the identities and (b) incorporates a concept of ownership in which access rights for a system resource may be granted and revoked by the entity that owns the resource.	IETF RFC 4949
Diversity	The differences presented when comparing two or more security measures, in terms of functionality, technology and code.	ED-203A/DO-356A
Domain (Aircraft)	A set of equipment and related networks that share common administrative, security, and functional attributes.	ARINC 664 P5
	Logical environment that allocates and separates resources for the simultaneous operation of the system and host platform.	ARINC 811
Elemental Analysis	Elemental analysis method provides a measurement of the verification process to support the determination of verification. coverage and completeness. Every functional element within the FFP (Functional failure path) is identified and verified using verification test cases that meet the verification objectives.	ED-80/DO-254

Term	Definition	Source
Effectiveness (Security) see also Security Effectiveness	The ability of a security countermeasure to reduce the occurrence of successful attacks.	ED-202A/DO-326A
	The ability of a security measure to prevent, mitigate, detect, react to or recover from successful attacks on assets, while permitting and preserving the intended use of the assets.	ED-203A/DO-356A
	A property of a TOE representing how well it provides security in the context of its actual or proposed operational use.	IETF RFC 4949
Electronic Distribution of Software	Electronic airborne software distribution or Electronic Distribution of Software (EDS) is the process of electronically moving software and data from one location to another location, wired or wirelessly, without the use of portable electronic media such as magnetic disks, optical disks, or flash drives. See ARINC Report 827 for description of EDS.	ED-204A/DO-355A
Encryption	Cryptographic transformation of data (called “plain text”) into a form (called “cipher text”) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption”, which is a transformation that restores encrypted data to its original state.	IETF RFC 2828, IETF RFC 4949
Equipment	Aircraft, system, item, or component of an item, or any aggregate thereof.	ED-203A/DO-326A
Evaluation Assurance Level (EAL)	Set of assurance requirements that represents a point on the Common Criteria predefined assurance scale.	CNNSI 4009-2015
Event	Occurrence or change of a particular set of circumstances. ***NOTE 1 TO ENTRY:*** *An event can be one or more occurrences, and can have several causes.* ***NOTE 2 TO ENTRY:*** *An event can consist of something not happening.* ***NOTE 3 TO ENTRY:*** *An event can sometimes be referred to as an “incident” or “accident”.*	ISO/IEC 27000:2018 ED-205 refers to ISO 27000 2016 same definition
Exposed Vulnerability	A security vulnerability within a function or system that is available for exploit by an attacker.	ED-204A/DO-355A
External (Aircraft)	A reference outside of aircraft systems. Note that this includes reference to systems on other aircraft and to systems that may be carried onboard but are not considered part of the aircraft type configuration. See System (Aircraft) and External Dependencies.	ED-202A/DO-326A
External Agreement	Expresses the trust placed in an external interfaces, such as contracts, service level agreements, etc.	ED-201

Term	Definition	Source
	Assumptions and requirements for the purpose of coordinating roles and responsibilities between dependent systems and external actors.	ED-202A/DO-326A ED-204A/DO-355A
External Dependencies (Aircraft)	Assumptions about the physical and logical sphere of control outside the asset, such as legislation or regulation.	ED-201
	Features of external information systems which can affect the function, including interfaces, dataflows, security countermeasures, and plans and procedures. Also see Dependent Systems.	ED-203A/DO-326A
External Population	Those persons, organizations, or external systems which can interact with the assessment asset under expected conditions of operation and/or failure.	ED-202A/DO-326A
Failure Condition	A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.	AMC 25.1309 (CS-25 Amendment 24)
Field Loadable Software (FLS)	FAA 8110.49 defines Field Loadable Software as follow: Software that can be loaded without removal of the equipment from the installation. FLS can also refer to either executable code or data (see EUROCAE ED-12B / RTCA DO-178B). FLS might also include software loaded into a line replaceable unit at a repair station or shop.	ARINC 667-1
Final Assessment	A systematic, comprehensive evaluation of an implemented system to show that relevant objectives and requirements are met.	inspired by: SAE ARP 4761, “Functional Hazard Assessment”
Firewall	An internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be “inside” the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be “outside” the firewall).	IETF RFC 2828, IETF RFC 4949
Flight Safety Hazard	A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof.	SAE ARP 5150, “Hazard”
Forensic Analysis	The practice of analyzing the computer-related data for investigative purposes in a manner that maintains the integrity of the data.	CNNSI 4009-2015 “Forensics”
Function	Intended behavior of a product based on a defined set of requirements regardless of implementation.	ED-79A / ARP4754A

Term	Definition	Source
General Management	Executive management person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organisation ***NOTE 1 TO ENTRY:*** *Executive management is sometimes called top management and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar role.*	ISO/IEC 27000:2016 ED-205
Ground Support Information System (GSIS)	Ground Support Information Systems (GSIS) are Ground Systems that are used to accomplish the process of Data Distribution and storage of Airborne Software and Data. Systems for creation and modification of UMS and UCS are also in the scope of Ground Support Information Systems.	ED-204A/DO-355A
Ground Support Equipment (GSE)	Refers to Ground Support Equipment that digitally connects to the aircraft at any time during ground or maintenance operations.	ED-204A/DO-355A
Hardware Controlled Software (HCS)	All airborne software which is configuration managed by the hardware part number of the hardware which contains the software is considered Hardware Controlled Software (HCS).	ED-204A/DO-355A
Identity	Information that is unique within a security domain and which is recognized as denoting a particular entity of that domain.	NIST SP800-27 (Withdrawn)
	The set of physical and behavioral characteristics by which an individual is uniquely recognizable. Source: FIPS PUB 201-1 ***NOTE:*** *This also encompasses non-person entities (NPEs).*	CNNSI 4009 - 2015
Impact	Damage or costs to an organization caused by an information security event.	ED-201
Independence	A concept that minimizes the likelihood of common vulnerabilities and propagation of attacks between security measures.	ED-79A/ARP4754A
Incident	A failure to meet an Information Security objective potentially resulting from an attack. (Ed.: see also “Security Incident”).	ED-202/DO326
Information	Information is the (subjective) interpretation of data.	Gollmann, 2005
Information Assurance	An attribute of an information system that provides grounds for having confidence that the system operates such that the system security policy is enforced.	IETF RFC 2828, IETF RFC4949 “assurance”

Term	Definition	Source
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability, Source: 44 U.S.C. Sec 3542.	CNNSI 4009-2015 ED-203A/DO-356A/ED-205 refer NIST SP800-53, Rev 2 Same definition
	Preservation of confidentiality, integrity and availability of information Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.	(ISO/IEC 27000:2018) ED-205
	Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)	ED-203A/DO356A ED-204A/DO-355A referring to Title 44 U.S.C., §3542
Information Security Threat	See “Intentional Unauthorized Electronic Interaction”.	ED-202A/DO-326A
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Ed.: See also Title 44 U.S.C, Sec 3502).	NIST SP800-53, Rev.5
Information Security Management System (ISMS)	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. ***NOTE:*** *The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.*	ISO/IEC 27000, 2005
Instruction for Continued Airworthiness	Instructions for Continued Airworthiness are the instructions and information that are necessary for the continued airworthiness of the aircraft, engine, propeller, parts and appliances, which are required in accordance with the applicable Certification Basis or Standard to be developed and/or referenced by the Design Approval Holder. (Source: EASA CM No.: CM–ICA-001 Issue 01 issued 02 May 2017, Section 1.4)	ED-204A/DO-355A
In-service security	In-service security evaluation refers to all activities, which are carried out subsequent to the release of a product into service, with the objective to confirm that the security effectiveness is still compliant with the relevant requirements.	ED-203A/DO-356A

Term	Definition	Source
Integrator Guidance	Specifications and technical and organizational requirements for the secure operation and maintenance of a system or item by an aircraft integrator or operator. These are the restrictions or requirements on the policies and procedures needed to satisfy the security requirements and should include all relevant requirements involving use, administration, installation, maintenance, or disposal. See also “User Guidance”.	ED-202A/DO-326A
Integrity	**Security usage:** Safeguarding the accuracy and completeness of information and processing methods	ED-205 ISO17799 withdrawn)
	Safety Usage: Qualitative or quantitative attribute of a system or an item indicating that it can be relied upon to work correctly. It is sometimes expressed in terms of the probability of not meeting the work correctly criteria.	ED-79A / ARP4754A
Intended actions	Operational action or sequence of actions undertaken to interact with the assessment asset which the requirements intend to occur. Examples include access / manipulation / modification / deletion / creation / administration / maintenance / installation.	ED-202A/DO-326A
Intentional Unauthorized Electronic Interaction	A circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this includes malware and the effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic jamming. (Ed: see also Information Security Threat).	ED-202A/DO-326A
	A circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. This includes the consequences of malware and forged data and the effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic disturbance.	ED-203A/DO-356A
Intrusion Detection	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network.	NIST SP800-94
	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.	NIST SP800-94
Intrusion Detection System (IDS)	Software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.	NIST SP800-94
	Software that automates the intrusion detection process.	NIST SP800-94

Term	Definition	Source
Isolation	Physical or logical boundaries between security measures or functions intended to ensure that compromise or failure of one security measure or function (or of a shared resource) does not affect another security measure or function.	ED-203A/DO-356A
Item (Aircraft)	A hardware or software element having bounded and well-defined interfaces.	ED-79A / ARP4754A
Key Management	The process of handling keying material during its life cycle in a cryptographic system; and the supervision and control of that process. (See: key distribution, key escrow, keying material, public-key infrastructure.) Usage: Usually understood to include ordering, generating, storing, archiving, escrowing, distributing, loading, destroying, auditing, and accounting for the material.	IETF RFC 2828, IETF RFC 4949
Level of Risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.	ISO/IEC 27000:2018 (ED-205 refers to 27000:2016 same definition)
Level of Threat	A qualitative evaluation of the possibility that a Threat Condition might occur.	ED-202A/DO-326A
Likelihood	A classification of how often an event can be expected to occur across a given operational span.	ED-202A/DO326A
	The chance of something happening.	ISO/IEC 27000:2018 ED-205 refers to ISO/IEC 27000:2016 same definition)
Malware	Malicious software that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.	adapted from NIST SP800-83
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.	NIST SP800-53, Rev.2
Management system	A structured set of interdependent processes, documents and principles that are intended to ensure that the activities of an organisation are directed, planned, conducted and controlled in such a way to provide reasonable assurance that the objectives of the organisation are met. Examples of management systems include Safety, Security, Quality, Requirement etc.	ED-205

Term	Definition	Source
Mandatory Access Control (MAC)	An access control service that enforces a security policy based on comparing (a) security labels (which indicate how sensitive or critical system resources are) with (b) security clearances (which indicate system entities are eligible to access certain resources).	IETF RFC 2828, IETF RFC 4949
Media	Devices or material, which acts as a means of transferring or storage of software (e.g., programmable read-only memory, magnetic tapes or discs).	ARINC 667-1 ED-204A/DO-355A
	Physical devices or writing surfaces including magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but excluding display media) onto which information is recorded, stored, or printed within an information system.	NIST SP800-53, Rev.5 (ED-203A refers to Rev 2 same definition)
Misuse (Security)	Unintended (according to the design intent) actions undertaken by a person or system to interact with systems, interfaces, or data. See Use.	ED-202A/DO-326A
Mitigation	Reduction of risk either through lessening of impact or lessening of occurrence.	ED-202A/DO-326A
Multi-Item	An item that includes more than one item (e.g. a software/hardware package which includes multiple software/hardware components with potentially differing assurance levels).	ED-203A
Non-repudiation	Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.	NIST SP800-53, Rev.5
	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information [Source: CNSSI No. 4009]	ED-203A/DO-356A
Objective (Process)	A statement of intent to ensure that identified properties will hold for the outputs of a process. The process objectives need not be goals of the process itself, but may be a consequence of the goals and activities of the process.	ED-202A/DO-326A
Operational conditions	A condition of the aircraft which can result from operational events.	ED-202A/DO-326A
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). [FIPS200]	FIPS200 NIST SP800-53, Rev.2

Term	Definition	Source
Operational environment	The set of defined concepts of operations, regulations, plans, policies, and procedures of the external organizations and systems that interact with the dependent systems of the aircraft, together with any regulations and policies which apply internally to the aircraft systems themselves.	ED-202A/DO-326A ED-204A/DO-355A
Operational events	Events that are part of the intended function and operation of the aircraft.	ED-202A/DO-326A
Operational Security Measures	Security measures that [are] applied during the operation of the aircraft.	ED-204A/DO-355A
Operational span	The exposure of an aircraft type to the information security threat considered both over multiple aircraft and time.	ED-202A/DO-326A
Operational Security Measures	Security measures that [are] applied during the operation of an aircraft.	ED-204A/DO-355A
Operations	In any architectural context, when two or more elements cooperate to achieve a stated objective, that objective is an operation.	ED-202A/DO-326A
Operator	The operator is the organization that operates an aircraft or is responsible of the maintenance of the aircraft.	ED-204A/DO-355A
Operator Guidance	Specifications and technical and organizational requirements for the secure preparation, use, and administration of an aircraft and aircraft systems by an operator. These are the restrictions or requirements on the policies and procedures needed to satisfy the security objectives and should include all relevant requirements involving use, administration, installation, maintenance, or disposal.	ED-202A/DO-326A
Penetration Test	A method for gaining assurance in the security of a system by attempting to breach some or all of that system's security, using the same tools and techniques that an attacker might use.	ED-205
Principle	A comprehensive and fundamental law, doctrine, or assumption.	ED-203A/DO356A
Protection Profile	An implementation-independent set of security requirements for a category of systems that meet specific user needs.	adapted from: ISO/IEC 15408-1:1999

Term	Definition	Source
Public Key Certificate	A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date). In the information assurance (IA) community, certificate usually implies public key certificate and can have the following types: A digital representation of information which at least (a) identifies the certification authority issuing it, (b) names or identifies its subscriber, (c) contains the subscriber's public key, (d) identifies its operational period, and (e) is digitally signed by the certification authority issuing it.	NIST SP800-32; CNNSI No 1300 “Certificate”
Public Key Infrastructure (PKI)	PKI is a set of policies, processes, server platforms, software, and workstations used to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke digital certificates.	NIST SP800-32
Refutation	Refutation acts as an independent set of assurance activities beyond analysis and requirements. As an alternative to exhaustive testing, refutation can be used to provide evidence that an unwanted behavior has been precluded to an acceptable level of confidence.	ED-203A/DO-356A
Reliability	**Security usage:** The ability of a system to perform a required function under specified conditions for a specified period of time.	IETF RFC 2828, IETF RFC 4949
	Safety use: The probability that an item will perform a required function under specified conditions, without failure, for a specified period of time.	ED-79A / ARP4754A
Requirement	An identifiable element of a function specification (technical) or a development assurance standard (assurance) that can be validated and against which an implementation can be verified.	ED-202A/DO-326A
	An identifiable element of a function specification that can be validated and against which an implementation can be verified.	ED-79A / ARP4754A
Response Centres	An organization or unit which receives reports of incidents and vulnerabilities and analyses them to produce alerts and mitigation advice.	ED-201
Residual Risk	Risk remaining after risk treatment ***NOTE 1 TO ENTRY:*** *Residual risk can contain unidentified risk.* ***NOTE 2 TO ENTRY:*** *Residual risk can also be known as “retained risk”.*	ISO/IEC 27000:2018 ED-205 (ED-205 refers to ISO/IEC 27000:2016 same definition)
Risk (security)	Exposure to the possibility of harm. The risk of an event is a function of the severity of the adverse event and the level of threat of that event.	ED-202A/DO-326A

Term	Definition	Source
	effect of uncertainty on objectives (3.49) ***NOTE 1 TO ENTRY:*** *An effect is a deviation from the expected — positive or negative.* ***NOTE 2 TO ENTRY:*** *Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.* ***NOTE 3 TO ENTRY:*** *Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.* ***NOTE 4 TO ENTRY:*** *Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.* ***NOTE 5 TO ENTRY:*** *In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.* ***NOTE 6 TO ENTRY:*** *Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.*	ISO/IEC 27000:2018 (ED-205)
	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence	NIST SP 800-53, Rev 5
	The level of impact on operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [FIPS 200]	ED-205 adapted from: NIST SP 800-53, Rev 2
Risk Acceptance	Informed decision to take a particular risk ***NOTE 1 TO ENTRY:*** *Risk acceptance can occur without risk treatment or during the process of risk treatment* ***NOTE 2 TO ENTRY:*** *Accepted risks are subject to monitoring and review.*	ISO/IEC 27000:2018 (ED-205) (ED-205 refers to ISO/IEC 27000:2016 same definition)

Term	Definition	Source
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk ***NOTE 1 TO ENTRY:*** *Risk analysis provides the basis for risk evaluation and decisions about risk treatment* ***NOTE 2 TO ENTRY:*** *Risk analysis includes risk estimation.*	ISO/IEC 27000:2018 (ED-205) (ED-205 refers to ISO/IEC 27000:2016 same definition)
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation	ISO/IEC 27000:2018 (ED-205) (ED-205 refers to ISO/IEC 27000:2016 same definition)
Risk Communication and Consultation	Set of continual and iterative processes (3.54) that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders (3.37) regarding the management of risk (3.61) ***NOTE 1 TO ENTRY:*** *The information can relate to the existence, nature, form, likelihood (3.41), significance, evaluation, acceptability and treatment of risk.* ***NOTE 2 TO ENTRY:*** *Consultation is a two-way process of informed communication between an organization (3.50) and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is — a process which impacts on a decision through influence rather than power; and an input to decision making, not joint decision making.*	ISO/IEC 27000:2018 (ED-205)

Term	Definition	Source
	Continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk NOTE 1 TO ENTRY: The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk, NOTE 2 TO ENTRY: Consultation is a two-way process of informed communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is • a process which impacts on a decision through influence rather than power and • an input to decision making, not joint decision making	ISO/IEC 27000:2016 (ED-205)
Risk Criteria	Terms of reference against which the significance of risk is evaluated ***NOTE 1 TO ENTRY:*** *Risk criteria are based on organisational objectives, and external and internal context* ***NOTE 2 TO ENTRY:*** *Risk criteria can be derived from standards, laws, policies and other requirements*	ISO/IEC 27000:2018 (ED-205) (ED-205 refers to ISO/IEC 27000:2016 same definition)
Risk Identification	Process of finding, recognising and describing risks ***NOTE 1 TO ENTRY:*** *Risk identification involves the identification of risk sources, events, their causes and their potential consequences.* ***NOTE 2 TO ENTRY:*** *Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.*	ISO/IEC 27000:2018 (ED-205) (ED-205 refers to ISO/IEC 27000:2016 same definition)
Risk Management	The continuous process of identifying, controlling, and mitigating problems according to their risk as identified through risk assessment.	ED-202A/DO-326A
	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. [FIPS 200]	NIST SP 800-53, Rev 2 (ED-205)

Term	Definition	Source
	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.	NIST SP 800-53, Rev 5
	The (continuous) process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.	ENISA Risk Management Glossary
Risk management process	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. [FIPS 200]	NIST SP 800-53, Rev 2 (ED-205)
Risk Treatment	Process to modify, avoid, transfer or retain risk.	ED-205 Adapted from NIST SP 800-160
Role	Predefined set of rules establishing the allowed interactions between a user and the Target of Evaluation.	Common Criteria 2.2, Part 1
Role Based Access Control (RBAC)	A form of identity-based access control wherein the system entities that are identified and controlled are functional positions in an organization or process.	IETF RFC 2828, IETF RFC 4949
Safety Architecture	That aspect of the architecture which is concerned with the concepts and basic methods for satisfying the safety objectives and requirements. A safety architecture defines architectural elements, together with their roles, responsibilities and interrelationships that will support the safety objectives. Elements may incorporate hardware, software, algorithms, procedures, and policies.	ED-202A/DO-326A
Safety Function	The part of the organisation responsible for safety activities.	ED-205
Safety Register	Record of information about identified safety risks.	ED-205
Scale of threat	the expectation that a threat will materialize.	ED-201

Term	Definition	Source
Security	The purpose of security is ensuring the safety of flight and maintaining operation of civil aviation infrastructure without disruption.	ED-201
Security Assurance	The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given security requirements.	ED-79A/ARP 4754A
Security Architecture	That aspect of the architecture which is concerned with the concepts and basic methods for satisfying the security requirements. A Security architecture defines architectural elements, together with their roles, responsibilities and interrelationships, which will implement and support the security measures. Elements may incorporate hardware, software, algorithms, procedures, and policies.	ED-202A/DO-326A
Security Audit	An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and ... procedures, ... detect breaches in security services, and recommend any ... changes that are indicated for countermeasures.	adapted from ISO 7498-2, "security audit"
Security Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.	adapted from NCSC TG-004
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.	NIST SP800-53, Rev. 5
	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]	NIST SP800-53, Rev. 2 (ED-205)
Security Effectiveness	The ability of the security measure to mitigate misuse of the assets by the unauthorized elements of the external population, while permitting and preserving use of the assets by the authorized elements of the external population. [Ed.: see also Effectiveness (Security)]	ED-202A/DO-326A
Security Effectiveness Objective	A statement of intent to achieve a level of security effectiveness against a specified security environment.	ED-202A/DO-326A
Security Environment	A security environment is the external security context in which an asset performs its function. For an aircraft, or system of an aircraft, the aircraft/system security environment is characterized by the set of security assumptions outside the control of the aircraft/system developer which are used in the safety assessment of the aircraft/system.	ED-202A/DO-326A

Term	Definition	Source
Security Event	A security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.	Adapted from ISO 27000:2018 Information security event (ED-204A/ DO-355A)
	Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls (3.14), or a previously unknown situation that can be security relevant.	ISO27000:2018 "Information security event"
	A security event is an action directed against a function with the intent to cause a security relevant change of state of function. A security event may require investigation to check whether it was legitimate or unwanted. An unwanted security event is a security incident. A security event may be intentional or inadvertent.	ED-204A/DO-355A
	An occurrence in a system that is relevant to the security of the system.	IETF RFC 2828, IETF RFC 4949
Security Function	The part of the organisation responsible for security activities.	ED-205
Security Incident	A single or a series of unwanted or unexpected information security events that could potentially affect aviation safety. [Source: adapted from ISO27000]	Adapted from ISO 27000:2018 Information Security Incident (ED-204A/DO-255A)
	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.	ISO/IEC 27000:2018 "Information security incident"
Security Management System (SeMS)	A structured approach to managing security as an integral part of its overall business, systematically integrating security risk management into an organization's day-to-day operations in close alignment with other risk management systems.	adapted from ICAO Doc 8973
Security Measure	Used to mitigate or control a threat condition. Security measures may be features, functions, or procedures, both onboard or offboard. Security measures can be technical, operational, or management.	ED-202A/DO-326A

Term	Definition	Source
Security Objective	A statement of intent to counter identified threats and/or to satisfy identified organization security policies and assumptions.	Common Criteria 2.2, Part 1
Security Perimeter	The security perimeter is the boundary between an asset's internal security context and its security environment.	ED-202A/DO-326A
Security Policy	A set of criteria for the provision of security services. SP 800-160-1 adapted A set of rules that governs all aspects of security-relevant system and system component behavior.	NIST SP800-53, Rev.5
	The statement of required protection of information.	NIST SP800-27
Security Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Ed.: see also "Risk"]	NIST SP800-53, Rev.5 "risk"
Security Risk Register	Record of information about identified security risks.	ED-205
Security Target	A set of security requirements and specifications to be used as the basis for evaluation of an identified Target of Evaluation. [This term is specific to the Common Criteria]	Common Criteria 2.2, Part 1
	An implementation-dependent statement of security needs for a specific identified Target of Evaluation. [This term is specific to the Common Criteria]	derived from Common Criteria 3.1, Part 1
Severity	Qualitative indication of the magnitude of the adverse effect of a threat condition.	ED-202A/DO-326A
Software	Data or code (executable or not) that defines controls or is used by its target hardware to perform its function.	ARINC 667
Structural coverage analysis	An evaluation of the code structure, including interfaces, exercised during requirements-based testing.	ED-12C / DO-178C
Supplier Controlled Software	The supplier of this type of software is the TC/STC holder or the developer of the software. Changes to Supplier Controlled Software (SCS) require approval by the certification authority. [Source ARINC 667]	ARINC 667-1 (ED-204A/DO-355A)

Term	Definition	Source
System (Aircraft)	A combination of inter-related items arranged to perform a specific function(s).	ED-79A / ARP4754A
System (Information)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. ***NOTE:*** *Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. [Title 44 U.S.C, Sec 3502]*	CNNSI 4009-2015 "Information System" (ED-203A/DO-356A)
	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note that information systems consist of people, processes, and technology. [Title 44 U.S.C, Sec 3502] [Source: NIST SP800- 53, Rev.2 "Information System"]	NIST SP800- 53, Rev.2 "Information System" ED-203A/DO-356A
System (Security)	An item or collection of items arranged to perform a specific function(s) which has a well-defined security environment.	ED-202A/DO-326A
System Hardening	The process of securing a system by reducing its surface of vulnerability. Reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.	ED-204A/DO-355A
Target	The destination of the attack associated with a specific threat scenario.	ED-203A/DO-356A
Target of Evaluation (ToE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. [This term is specific to the Common Criteria]	Common Criteria 2.2, Part 1
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [FIPS 200]	NIST SP800-53, Rev.2
Technical Vulnerability Management	Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems however it can also extend to organizational behavior and strategic decision-making processes. Refer also to ISO 27001/27002.	ED-204A/DO-355A
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	NIST SP800-53, Rev.5

Term	Definition	Source
	Potential cause of an unwanted incident, which can result in harm to a system or organization.	ISO/IEC 27000:2018 (ED-205 refers to ISO/IEC 27000:2016 same definition)
	A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.	IETF RFC4949
Threat agent	see Threat Source	
Threat Condition	A condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more acts of intentional unauthorized electronic interaction, involving cyber threats, considering flight phase and relevant adverse operational or environmental conditions. Also see failure condition.	ED-202A/DO-326A
Threat Scenario	The specification of intentional unauthorized electronic interaction, consisting of the contributing threat source (attacker and attack vector), vulnerabilities, operational conditions, and resulting threat conditions, and events by which the target was attacked.	ED-202A/DO-326A
	The description of a threat exploiting a certain vulnerability or set of vulnerabilities to attack assets leading to adverse impacts.	ICAO RCS
Threat Source	Any human user or Information Technology (IT) product or system, which may attempt to violate the security policy and perform an unauthorized operation with the system.	adapted from: NIAP CIM-BRE
	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may mistakenly trigger a vulnerability. The threat source of a threat is intent and method: the attacker and the attack vector.	ED-202A/DO-326A
	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.	CNSS Instruction No. 4009
Token	**1.** **Access control usage:** An object that is used to control access and is passed between cooperating entities in a protocol that synchronizes use of a shared resource. Usually, the entity that currently holds the token has exclusive access to the resource. **2.** **Authentication usage:** A data object or a physical device used to verify an identity in an authentication process. **3.** **Cryptographic usage:** A portable, user-controlled, physical device (e.g., smart card or PCMCIA card) used to store cryptographic information and possibly also perform cryptographic functions.	IETF RFC 2828

Term	Definition	Source
	Access control usage: An object that is used to control access and is passed between cooperating entities in a protocol that synchronizes use of a shared resource. Usually, the entity that currently holds the token has exclusive access to the resource. **Authentication usage**: A data object or a physical device used to verify an identity in an authentication process. (deprecated - use definition "authentication information" instead) **Cryptographic usage**: (deprecated - replaced by definition of "cryptographic token")	IETF RFC 4949
Trust Anchor	A Trust Anchor (also known variously as a Certificate Authority Certificate or a Root Certificate) is a certificate that is used as the basis for verifying the digital signature of a certificate, or for validating a chain of certificates.	ATA Spec 42: 2018 5-13-1
Trusted Area	Physical location where there is no threat against the asset (FLS, PDL, PMAT, etc.).	ED-204A/DO-355A
Trust Relationship	The relationship whereby an external population can interact with the assessment asset. There is a trust relationship whenever an external population can use or misuse an asset.	ED-202A/DO-326A
Unauthorized Interaction	see Intentional Unauthorized Electronic Interaction	ED-202A/DO-326A
Use (Security)	Intended actions undertaken by the external population to interact with aircraft systems, interfaces, or data, in order to perform intended duties. See Misuse.	ED-202A/DO-326A
User Certifiable Software (UCS)	When this software is modified, it should be reviewed and approved by the appropriate Airworthiness Certification Office.	ARINC 667-1
User Modifiable Software (UMS)	This is software that is intended for modification by the aircraft operator (airline) without review by the certification authorities, the airframe manufacturer, or the equipment vendor. A tool is usually provided so the software can only be modified within given boundaries.	ARINC 667-1
Validation	The determination that the requirements for a product are correct and complete. [Are we building the right aircraft/ system/ function/ item?]	ED-79A / ARP4754A
Verification	The evaluation of an implementation of requirements to determine that they have been met. [Did we build the aircraft/ system/ function/ item right?]	ED-79A / ARP4754A

Term	Definition	Source
Verification elements	Details to describe how the verification activity is performed. Depending on the verification method (e.g. test, inspection, analysis, ...) different details need to be described. For example the verification elements for verification by tests are the test cases, tests procedures, tests results,…	ED-203A/DO-356A
Victim	An intermediate element of a threat scenario which does not contribute to the protection against the attack and is not a target of this attack.	ED-203/DO-356
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.	NIST SP800-53, Rev 5 (ED-203A/DO-356A/ED-205 refer to NIST SP800-53, Rev 2 same definition)
	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.	ED-202A/DO-326A DO-204A/DO-355A
Vulnerability Assessment	Generic term encompassing the two existing methods, namely vulnerability analysis or vulnerability testing, used during the evaluation of the development and anticipated operation of the aircraft/ system/ item that could be exploited by a threat source.	ED-202A/DO-326A
Vulnerability Dossier	Listing, analysis, and classification of abnormalities and threats determined as vulnerabilities through analysis and vulnerability testing according to a security risk assessment.	ED-202A/DO-326A
Vulnerability Testing	Methods for testing for unintended function and robustness, using exploratory testing methods to detect and probe vulnerabilities that can be present in an implementation and attempts to break or to circumvent the security measures.	ED-202A/DO-326A
Well-known Vulnerability	A vulnerability that has been documented during previous use of some portion of the system, and the documentation is known and available to the developer.	ED-202A/DO-326A
Whitelist (WL)	A whitelist is a computer file that lists all authorized digital certificates that have permission to access to a certain system or protocol. Any entity that is not included in the Whitelist has its access, to the system or protocol, denied.	ED-204A/DO-355A

TABLE 2: REFERENCES

Identification	Reference
44 U.S.C. § 3502	Title 44, US Code, §3502, Currently available from: http://uscode.house.gov/search/criteria.shtml
44 U.S.C. § 3542	Title 44, US Code, §3542, Currently available from: http://uscode.house.gov/search/criteria.shtml
AMC 25.1309	EASA Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, Book 2, Amendment 16, Chapter 25.1309
Arinc 664P5	Arinc/ARINC, Arinc Specification 664P5, Aircraft Data Network, Part 5, Network Domain Characteristics and Interconnection, April 2005
Arinc 667-1	Arinc/AEEC, Arinc Report 811, Guidance for the Management of Field Loadable Software, November 2010
Arinc 811	Arinc/AEEC, Arinc Report 811, Commercial Aircraft Information Security Concepts of Operation and Process Framework, December 2005
Arinc 827	Arinc Report 827, Electronic Distribution of Software By Crate (EDS Crate), September 2010
ATA Spec 42	Airlines 4 America Spec 42, Aviation Industry Standards for Digital Information Security, Revision 2010
CC Part 1, Vers 3.1, Rev 4	Common Criteria, CC 3.1, Part 1, Revision 4, Sept 2006, Currently available from http://www.commoncriteriaportal.org/thecc.html
CNSS Instruction 4009	Committee on National Security Systems, National Information Assurance (IA) Glossary, No.4009, April 2015
DO-176B/C	RTCA DO-178B/C Software Considerations in Airborne Systems and Equipment Certification, 1992/2011
ENISA Risk Management Glossary	ENISA Risk Management Glossary, Available from: http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/glossary
Gollmann, 2005	Computer Security, 2nd edition, Dieter Gollmann, 2005, Wiley
GSA GSCH, 2004	General Services Administration (GSA), Government Smart Card Handbook, 2004, February 2004, Currently available from: http://www.smartcardalliance.org/resources/pdf/smartcardhandbook.pdf
Hansen, 1973	Brinch Hansen, Operating Systems Principles, 1973, Prentice Hall
ICAO Doc 4444	ICAO Doc 4444, 15th Edition, 2007, Air Traffic Management
ICAO Doc 8973	ICAO Doc 8973/9 Restricted, 9th Edition, 2014, Aviation Security Manual
ICAO Doc 9713	ICAO Doc 9713, 2th Edition, 2010, International Civil Aviation Vocabulary
ICAO Risk Context Statement (RCS)	ICAO Risk Context Statement (RCS), Restricted and Abridged (public) versions
IETF RFC2828	IETF, RFC2828, Internet Security Glossary, May 2000
IETF RFC4949	IETF, RFC4949, Internet Security Glossary, Version 2, August 2007
ISO 15408-1:2005	ISO/IEC 15408-1, Evaluation criteria for IT security, Part 1: Introduction and general model, October 2005
ISO 17799:2000	BS ISO/IEC 17799:2000, Security techniques - Code of practice for information security management , 2000
ISO 27000:2016	ISO/IEC 27000, Second Edition, Information security management systems - Overview and vocabulary, 2016
ISO 27000:2018	ISO/IEC 27000, Second Edition, Information security management systems - Overview and vocabulary, 2018
ISO 27001:2008	ISO/IEC 27001, Second Edition, Information security management systems - Requirements, 2008

Identification	Reference
ISO 27005:2011	ISO/IEC 27005, Security techniques - Information security risk management , 2011
ISO 7498-2:1989	ISO/IEC 7498-2, Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1989
ISO Guide 73	ISO Guide 73, Risk Management - Vocabulary, First Edition 2009
NIAP CIM-BRE	National Information Assurance Partnership (NIAP), Consistency Instruction Manual - Basic Robustness Environments, Release 2.0, March 2004, Currently available from: http://www.niap-ccevs.org/pp/ci_manuals.cfm
NIST SP800-12	NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, 1995. Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-27	NIST, Special Publication 800-27, Revision A, Engineering Principles for Information Technology Security, June 2004, Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-30	NIST, Special Publication 800-30, Risk Management Guide for Information Technology Systems, Jul 2002, Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-31	NIST, Special Publication 800-31, Intrusion Detection Systems, November 2001, http://everyspec.com/NIST/NIST-General/SP_800-31_30152/
NIST SP800-32	NIST, Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, Feb 2001, Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-37	NIST, Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004, Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-53	NIST, Special Publication 800-53 Rev.5, Recommended Security Controls for Federal Information Systems, Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-61	NIST, Special Publication 800-61, Computer Security Incident Handling Guide, January 2004, Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-83	NIST, Special Publication 800-83, Guide to Malware Incident Prevention and Handling, November 2005, Currently available from: http://csrc.nist.gov/publications/nistpubs
NIST SP800-94	NIST, Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007, Currently available from: http://csrc.nist.gov/publications/nistpubs
NSCS TG-004	National Security Agency, National Computer Security Center, NCSC-TG-004-88, October 1988
SAE ARP4754	SAE, ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, April 1996
SAE ARP4754A	SAE, ARP 4754A, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, December 2010
SAE ARP4761	SAE, ARP 4761, Guidelines and Methods for Conducting The Safety Assessment Process, December 1996
SAE ARP5150	SAE, ARP 5150, Safety Assessment of Transport Airplanes in Commercial Service, November 2003

This Page Intentionally Left Blank

APPENDIX A

WG-72 and SC-216 MEMBERSHIP

Chairpersons:

EUROCAE WG-72	Cyrille Rosay	EASA
RTCA SC-216	David Pierce	GE Aviation

Secretaries:

WG-72	Clive Goodchild	BAE Systems
SC-216	Sam Masri	Honeywell International, Inc.

Technical Programme Manager

EUROCAE	Anna Guégan

Program Director

RTCA	Karan Hofmann

First Name	Last Name	Company
Hannes	Alparslan	European Defence Agency (EDA)
Yohannes	Amare	The Boeing Company
Rosemberg	Andre da Silva	Agência Nacional de Aviação Civil (ANAC-Brazil)
John	Angermayer	The MITRE Corporation
Cyrille	Aubergier	SITAONAIR
Steven	Bates	Panasonic Avionics Corporation
Cristian	Bertoldi	AIRBUS SAS
Raphael	Blaize	APSYS
György	Blazsovszky	HungaroControl
Timo	Blunck	EUROCONTROL
Andy	Boff	Helios - UK
Liz	Brandli	Federal Aviation Administration (FAA)
Angelo	Bruno	LEONARDO SpA
Martin	Call	The Boeing Company
Jeffrey	Campbell	Department of National Defence of Canada
Cláudio	Castro	EMBRAER
Stephane	CHOPART	Airbus Helicopters
Philip	Church	Helios
Ernie	Condon	National Institute for Aviation Research (NIAR) at Wichita State University
Rosemberg	da Silva	ANAC - SAE
Brian	Daly	Transport Canada
Frédérique	Dauvillaire	THALES Groupe

Aharon	David	A.D.Ventures Software ltd.
Peter	Davis	CAA/SRG
Claudio	de Castro	Embraer
Gilles	Descargues	Thales Group
Alexander	Engel	EUROCAE
Zhe	Fan	COMAC BASTRI
Christian	Fiore II	The MITRE Corporation
Roman	Fischer	Skyguide
John	Flores	Federal Aviation Administration (FAA)
Joacy	Freitas	ANAC-Brazil
Patricia	Fuilla-Weishaupt	Airbus
Raoufou	Ganiou	Transport Canada
Eduardo	Garcia	CANSO
Marty	Gasiorowski	Worldwide Certification Services
Armelle	Gauthe	Airbus
Gilles	Gobbo	Airbus
Cesar	Gomez	Federal Aviation Administration (FAA)
Will	Gonzalez	Federal Aviation Administration (FAA)
Elena	Gromova	GOSNIIAS
Judicael	GROS-DESIRS	AIRBUS SAS
Edward	Hahn	Air Line Pilots Association (ALPA)
Jerry	Hancock	Inmarsat
Christian	Haury	Safran Electronics & Defense
Brian	Hoffman	Air Line Pilots Association (ALPA)
Mark	Kelley	AVISTA
Anne-Cecile	Kerbrat	Dassault Aviation
Varun	Khanna	Federal Aviation Administration (FAA)
Andrew	Kornecki	Embry-Riddle Aeronautical University
Marcus	Labay	Federal Aviation Administration (FAA)
Christopher	Lacey	AIRBUS SAS
Kristof	Lamont	EUROCONTROL
Laurent	Leonardon	Collins Aerospace
Jerome	Lephay	Collins Aerospace
Qi	Li	Department of National Defence
Marc	Lord	Transport Canada
Cyril	Marchand	Thales Group
Philippe	Marquis	Dassault Aviation
Andrew	McLaughlin	Honeywell International, Inc.

Peter	McNeely	Astronautics Corporation of America
Patrick	McTernen	American Airlines, Inc.
Kevin	Meier	Cessna Aircraft Company
Stephane	Miglio	Airbus
Dinkar	Mokadam	Association of Flight Attendants
Jean-Paul	Moreaux	European Aviation Safety Agency (EASA)
Cecile	Morlec	Airbus
Catherine	Morlet	European Space Agency
Joe	Morrissey	The MITRE Corporation
Patrick	Morrissey	Collins Aerospace
Michal	Mrazek	Honeywell International
David	Munoz	Thales Group
Ravi	Nori	Teledyne Control
Siobvan	Nyikos	The Boeing Company
Thomas	Obert	Airbus
Ted	Patmore	Delta Air Lines, Inc.
Mark	Perini	Honeywell International, Inc.
Tom	Phan	Federal Aviation Administration (FAA)
Aaron	Renshaw	American Airlines, Inc.
Philippe	Robert	PMV Engineering
Lionel	Robin	SAFRAN
Marc	Ronell	Federal Aviation Administration (FAA)
Chuck	Royalty	Aerospace Systems Cyber Security
Shohreh	Safarian	Federal Aviation Administration (FAA)
Romuald	Salgues	Airbus
Krishna	Sampigethaya	United Technologies Corporation
Michael	Schraub	DFS Deutsche Flugsicherung GmbH
Stefan	Schwindt	GE Aviation Systems UK
Remzi	Seker	Embry-Riddle Aeronautical University
Rebecca	Selzer	United Airlines, Inc.
Michael	Severson	Bell Helicopter Textron, Inc
Charles	Sheehe	NASA
Matt	Shreeve	Helios - UK (EUROCAE Member)
Peter	Skaves	Federal Aviation Administration (FAA)
Brittany	Skelton	The Boeing Company
Kristopher	Smith	Triumph Group
Stephen	Sterling	Department of National Defence of Canada
Seth	Stewart	ENSCO Avionics Inc.

Hugo	Teso	Emirates
Christian	Tettamanti	ACI EUROPE
Casey	Theisen	United Airlines, Inc.
Lirong	Tian	Aeronautics Computing Technique Research Institute (ACTRI)
Timothy	Tinney	Saab Group
Christophe	TRAVERS	DASSAULT AVIATION
Mitchell	Trope	Garmin Ltd.
Isidore	Venetos	Federal Aviation Administration (FAA)
Herman	Verhoef	IATA
Brian	Verna	Federal Aviation Administration (FAA)
Ivan	Vincze	HungaroControl
Anna	von Groote	EUROCAE
Tong	Vu	Federal Aviation Administration (FAA)
Mohammed	Waheed	Aviage Systems
Adrian	Waller	Thales Group
Jeffrey Jeng Hang	Wang	FLYING WHALES
Philip	Watson	Panasonic Avionics Corporation
Stephen	Williams	NATS
Matt	Winslow	Gulfstream Aerospace Corporation
Marcie	Wise	Delta Air Lines, Inc.
Thomas	Wittmann	ESG Elektroniksystem- und Logistik-GmbH
Cameron	Wright	Southwest Airlines Co
Dongsong	Zeng	The MITRE Corporation