



AEROSPACE STANDARD

AS9115™**REV. A**Issued 2010-04
Revised 2017-02

Superseding AS9115

Technically equivalent writings
published in all IAQG sectors.

(R) Quality Management Systems - Requirements for Aviation, Space, and
Defense Organizations - Deliverable Software (Supplement to 9100:2016)

RATIONALE

This standard supersedes the initial release of 9115 published in April 2010. This standard has been revised to incorporate the new clause structure and content of ISO 9001:2015. In addition, industry requirements, definitions, and notes have been revised in response to ISO 9001:2015 and 9100:2016 revisions and stakeholder needs.

This is the second revision of 9115 which is an international supplement to 9100 providing clarification of the corresponding 9100 requirements, as necessary, for deliverable software. In some cases, where clarification is needed, it was necessary due to the complexity of software to decompose "shall" statements in 9100 into more granular requirements. Where no software clarification is required of the 9100 requirements, the following phrase is presented: "The requirements of 9100 apply. No clarification required for software."

NOTE: This document must be used in conjunction with 9100:2016; references throughout the text to 9100 are understood to mean 9100:2016.

FOREWORD

This document standardizes, to the greatest extent possible, the software quality management system requirements for the aviation, space, and defense industry. This was accomplished through the harmonization of quality management system requirements from international aviation, space, and defense software standards and other applicable documents and good practice. The establishment of common requirements for use at all levels of the supply-chain by organizations around the world should result in improved quality, schedule, and cost performance by the reduction or elimination of organization unique requirements and wider application of good practice.

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2017 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
<http://www.sae.org>

SAE WEB ADDRESS:

Full document details: SAE AS9115A

SAE values your input. To provide feedback on this
Technical Report, please visit
<http://standards.sae.org/AS9115A>

Documents
Document Sharing Hub

TABLE OF CONTENTS

RATIONALE	1
FOREWORD	1
INTENDED APPLICATION	4
INTRODUCTION.....	4
0.1 General	4
0.2 Quality Management Principles	4
0.3 Process Approach	4
0.3.1 General	4
0.3.2 Plan-Do-Check-Act Cycle	4
0.3.3 Risk-Based Thinking	4
0.4 Relationship with Other Management System Standards	4
 QUALITY MANAGEMENT SYSTEMS – REQUIREMENTS	
1. SCOPE.....	5
2. NORMATIVE REFERENCES.....	5
3. TERMS AND DEFINITIONS.....	5
4. CONTEXT OF THE ORGANIZATION.....	9
4.1 Understanding the Organization and Its Context.....	9
4.2 Understanding the Needs and Expectations of Interested Parties	10
4.3 Determining the Scope of the Quality Management System.....	10
4.4 Quality Management System and Its Processes	10
5. LEADERSHIP	10
5.1 Leadership and Commitment.....	10
5.1.1 General.....	10
5.1.2 Customer Focus.....	10
5.2 Policy.....	10
5.2.1 Establishing the Quality Policy.....	10
5.2.2 Communicating the Quality Policy	10
5.3 Organizational Roles, Responsibilities, and Authorities	10
6. PLANNING	10
6.1 Actions to Address Risks and Opportunities.....	10
6.2 Quality Objectives and Planning to Achieve Them.....	11
6.3 Planning of Changes.....	11
7. SUPPORT	11
7.1 Resources	11
7.1.1 General.....	11
7.1.2 People	11
7.1.3 Infrastructure	11
7.1.4 Environment for the Operation of Processes.....	11
7.1.5 Monitoring and Measuring Resources	12
7.1.6 Organizational Knowledge	12
7.2 Competence.....	12
7.3 Awareness	12
7.4 Communication	12
7.5 Documented Information.....	12
7.5.1 General.....	12

7.5.2	Creating and Updating	12
7.5.3	Control of Documented Information	12
8.	OPERATION	13
8.1	Operational Planning and Control	13
8.1.1	Operational Risk Management	14
8.1.2	Configuration Management	14
8.1.3	Product Safety	15
8.1.4	Prevention of Counterfeit Parts	15
8.2	Requirements for Products and Services	15
8.2.1	Customer Communication	15
8.2.2	Determining the Requirements for Products and Services	15
8.2.3	Review of the Requirements for Products and Services	15
8.2.4	Changes to Requirements for Products and Services	15
8.3	Design and Development of Products and Services	16
8.3.1	General	16
8.3.2	Design and Development Planning	16
8.3.3	Design and Development Inputs	16
8.3.4	Design and Development Controls	16
8.3.5	Design and Development Outputs	17
8.3.6	Design and Development Changes	17
8.4	Control of Externally Provided Processes, Products, and Services	17
8.4.1	General	17
8.4.2	Type and Extent of Control	18
8.4.3	Information for External Providers	18
8.5	Production and Service Provision	18
8.5.1	Control of Production and Service Provision	18
8.5.2	Identification and Traceability	20
8.5.3	Property Belonging to Customers or External Providers	20
8.5.4	Preservation	20
8.5.5	Post-Delivery Activities	21
8.5.6	Control of Changes	21
8.6	Release of Products and Services	21
8.7	Control of Nonconforming Outputs	21
9.	PERFORMANCE EVALUATION	22
9.1	Monitoring, Measurement, Analysis, and Evaluation	22
9.1.1	General	22
9.1.2	Customer Satisfaction	22
9.1.3	Analysis and Evaluation	22
9.2	Internal Audit	22
9.3	Management Review	22
9.3.1	General	22
9.3.2	Management Review Inputs	22
9.3.3	Management Review Outputs	23
10.	IMPROVEMENT	23
10.1	General	23
10.2	Nonconformity and Corrective Action	23
10.3	Continual Improvement	23
11.	NOTES	23
11.1	Revision Indicator	23
ANNEX A	BIBLIOGRAPHY	24
ANNEX B	AVIATION, SPACE, AND DEFENSE BIBLIOGRAPHY	25
FIGURE 1	RELATIONSHIP OF INFORMATION ASSURANCE, INFORMATION SECURITY, AND CYBERSECURITY	

INTENDED APPLICATION

The requirements of 9100 apply with the following clarification for software.

Organizations whose products are deliverable software or contain deliverable software should use the supplemental 9115 standard when planning and evaluating the software design, development, release, procurement, and management activities of the organization. The 9115 standard provides guidance to the requirements of 9100 when it is desired to add “deliverable software” to the organization’s 9100-registration certificate, and a greater depth of specificity and granularity to the requirements for assuring that the objectives of 9100 will be met for deliverable software.

NOTE: This document is independent of the life cycle models (e.g., waterfall, spiral, agile, evolutionary, incremental) or methodology (e.g., objected oriented design, unified modeling language).

INTRODUCTION

0.1 General

The requirements of 9100 apply. No clarification required for software.

0.2 Quality Management Principles

The requirements of 9100 apply. No clarification required for software.

0.3 Process Approach

The requirements of 9100 apply. No clarification required for software.

0.3.1 General

The requirements of 9100 apply. No clarification required for software.

0.3.2 Plan-Do-Check-Act Cycle

The requirements of 9100 apply. No clarification required for software.

0.3.3 Risk-Based Thinking

The requirements of 9100 apply. No clarification required for software.

0.4 Relationship with Other Management System Standards

The requirements of 9100 apply. No clarification required for software.

QUALITY MANAGEMENT SYSTEMS – REQUIREMENTS

1. SCOPE

The requirements of 9100 apply with the following clarification for software.

This standard supplements the 9100 standard requirements for deliverable software and contains quality management system requirements for organizations that design, develop, and/or produce deliverable software and services for the aviation, space, and defense industry. This includes, as required, support software that is used in the development and maintenance of deliverable software and services. The deliverable software may be stand-alone, embedded, mobile application, or loadable into a target computer.

This deliverable software may also be part of services (e.g., cloud environment, web hosted solutions or platforms).

Where the use of Hardware Description Language (HDL) or high order language is utilized as the design source of electronic hardware [e.g., Application Specific Integrated Circuit (ASIC), Programmable Logic Device (PLD)]; the organization and customer, and/or supplier shall agree on the extent of applicability of this supplement.

NOTE: For airborne electronic hardware guidance, see RTCA/DO-254 or EUROCAE ED-80. For operations requirements, see 9100 Section 8.

Where Commercial-off-the-Shelf (COTS) or non-developmental software is integrated into a deliverable product, the organization and customer shall agree on the extent of applicability of this supplement.

For the purposes of this document, the terms “product” and “software product” are considered synonymous.

For the purposes of this document, the term “services” may be considered a product.

2. NORMATIVE REFERENCES

The requirements of 9100 apply with the following clarification for software.

9100:2016 Quality Management Systems – Requirements for Aviation, Space, and Defense Organizations

NOTE: Documents referenced in this standard, other than the normative references (i.e., ISO 9000, ISO 9001, 9100), are listed in the supporting bibliographies (see Annexes A and B). For undated references, the latest edition of the referenced document (including any amendments) applies. The referenced documents are “informative” references; the requirements of these referenced documents do not add any additional requirements to this standard.

3. TERMS AND DEFINITIONS

For the purposes of this document, the terms and definitions given in 9100 and ISO 9000 apply. The following terms and definitions are included to support the understanding of this document.

3.1 Baseline

The approved, recorded configuration of one or more configuration items that thereafter serves as the basis for further development, and is changed only through change control documented information [see RTCA/DO-178 or EUROCAE ED-12].

3.2 Commercial-off-the-Shelf (COTS) Software

Commercially available applications sold by vendors through public catalog listings. COTS software is not intended to be customized or enhanced. Contract-negotiated software developed for a specific application is not COTS software [see RTCA/DO-178 or EUROCAE ED-12].

NOTE: COTS software is a type of non-developmental software.

3.3 Configuration Item

One or more hardware/software entities treated as a unit for configuration management purposes or software life cycle data treated as a unit for configuration management purposes [based on RTCA/DO-178 or EUROCAE ED-12].

3.4 Critical Items

The definition in 9100, clause 3.2, applies with the following clarification for software.

Critical items in software are those characteristics, requirements, or attributes that have been determined to be most important to achieve product realization (e.g., safety, maintainability, testability, usability, performance). For example, in the case of an aircraft's flight control system software, the response time could be elevated to a critical item to ensure overall performance characteristics are met; or if a project has customer specific testability requirements, cyclomatic complexity may become a critical item.

3.5 Cyclic Redundancy Check (CRC)

A type of function that takes a data stream of any length as an input and produces a value of a certain space (commonly a 32-bit integer) as an output. A CRC can be used to detect alteration of data during transmission or storage.

3.6 Digital Signature (also referred to as a Digital Signature Scheme)

A type of asymmetric cryptography used to express compliance with the security properties of a handwritten signature on paper.

3.7 Information Assurance (IA)

The set of activities needed to protect information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation including protection, detection, and reaction capabilities.

This includes activities conducted to reduce vulnerability of operational networks, Information Technology (IT), and computing equipment. Activities may include development of innovative and cost-effective ways to mitigate those vulnerabilities. IA may include actions to provide assured access, and transparent identification and authentication across the network or within systems of systems.

See Figure 1 for added clarity of related terms.

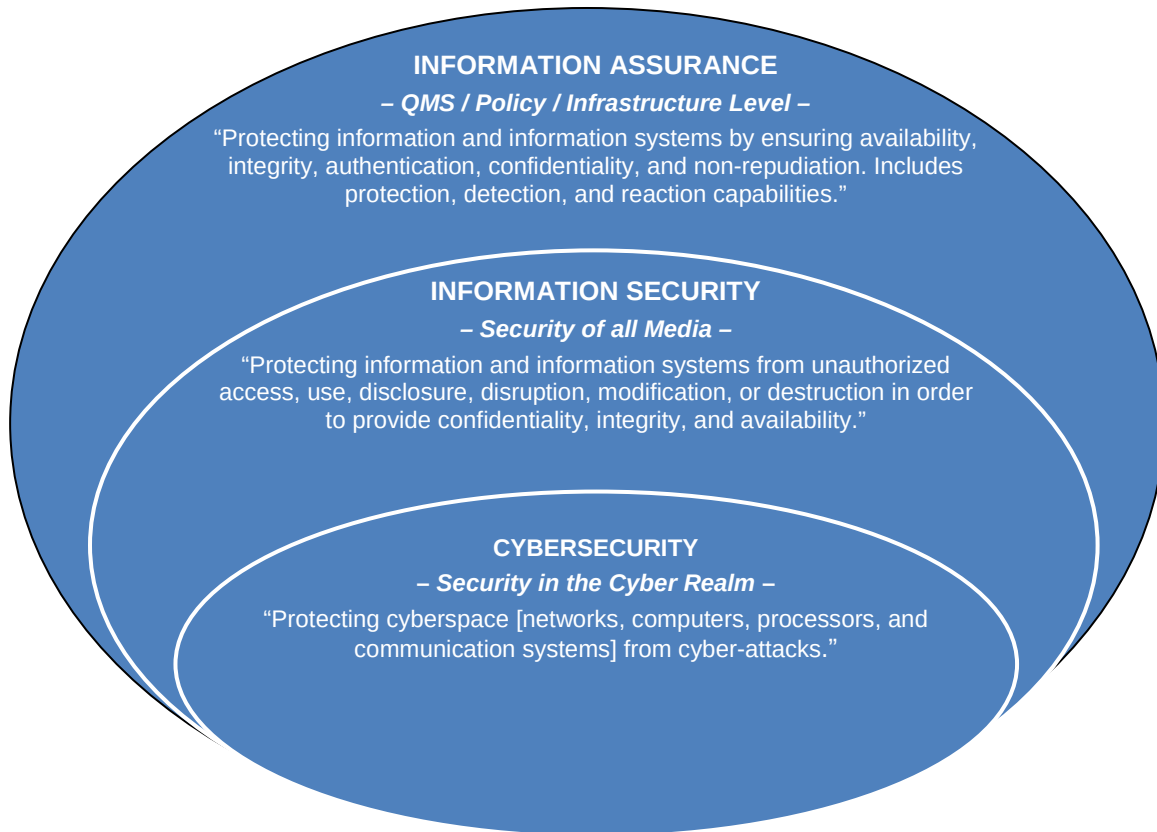


Figure 1 – Relationship of information assurance, information security, and cybersecurity

References:

- *Committee on National Security Systems National Information Assurance Glossary, CNSSI Instruction No. 4009 (26 April 2010)*
- *ISO 27001:2013 - Information technology – Security techniques – Information security management systems – Requirements*
- *ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security controls*
- *ISO 27034-1:2011 - Information technology – Security techniques – Application security – Part 1: Overview and concepts*

3.8 Interested Parties

A party having a right, share, or claim in a system or in its possession of characteristics that meet that party's needs and expectations [see ISO/IEC 12207].

NOTE: Interested parties include, but are not limited to customers, suppliers, regulatory bodies, and functional organizations or groups needed to achieve product quality.

3.9 Key Characteristic

The definition in 9100 (see clause 3.3) applies with the following clarification for software.

Key characteristics in software are those measurable attributes where variability can be measured by the project and can, if left unchecked, adversely impact the project or product in areas (e.g., memory utilization, response time, functionality, reliability, usability, efficiency, maintainability, portability).

3.10 Monitoring

The act of witnessing or inspecting selected instances of test, inspections, or other activities, or documented information of those activities, to assure that the activity is under control and that the reported results are representative of the expected results. Such activities could be performed and used as evidence for formal test verification to support conformity, certification, and customer acceptance.

Monitoring is usually associated with activities done over an extended period of time where 100% witnessing is considered impractical or unnecessary. Monitoring permits authentication that the claimed activity was performed as planned [see RTCA/DO-178 or EUROCAE ED-12].

3.11 Non-Developmental Software

Deliverable software that is not developed under the contract, but is provided by the organization, customer, or a third party [e.g., reused software, customer furnished software, COTS software, Government off-the Shelf (GOTS) software, open source software].

3.12 Phase

A collection of processes, activities, tasks, and outcomes within the software life cycle [see IEEE 24765].

3.13 Release

A particular version of a configuration item that is made available for a specific purpose (e.g., test release) [see ISO/IEC 12207].

3.14 Reliability

The probability of failure-free operation of a computer program in a specified environment for a specified time [based on IEEE 982.1].

NOTE: Software reliability requirements should consider the level and manner of fault and failure detection, isolation, fault tolerance, and recovery expected to be fulfilled by the software.

3.15 Robustness

The extent to which software can continue to operate correctly despite invalid inputs [see RTCA/DO-178 or EUROCAE ED-12].

NOTE: Robustness, in the software context, means that the organization has utilized techniques (e.g., exception handling, redundancy, related verification techniques).

3.16 Secure Hash Algorithm

Cryptographic functions that compute a fixed-length digital representation, known as a message digest, of an input data sequence of any length.