



Australian Government



CENTRE FOR DEFENCE INDUSTRY CAPABILITY



Defence Industry Qualifications and Requirements

July 2020

An overview of industry standards, certifications,
accreditations & compliance requirements

Table of Contents

How to use this booklet	2
Understanding general business qualifications and requirements	3
Do you have the required Occupational Health and Safety systems in place?	3
Do you need to consider environmental management?	3
Do you have a risk management plan?.....	3
How do you manage collaborative business relationships?.....	4
Are you pro-actively managing your assets?	4
Does your quality management system meet requirements to do business in the defence industry?.	5
What is the key quality management system required to work in the defence industry?	5
What other specific quality requirements might you need to consider?.....	5
Are you working in the aerospace industry?	8
Do you need to implement additional aerospace specific quality management?	8
What are the compliance requirements for the aerospace industry in key markets?.....	8
Understanding security requirements	10
What security requirements do you need to meet to supply to the defence market?	10
Have you assessed your information security?	10
What additional information security requirements do you need to meet to supply technology goods and services to the defence market?	11
Do you want to join global supply chains and export defence goods?	13
What standards do you need to meet to supply internationally?.....	13
Do you want to supply to the US aerospace and defence markets?.....	13
What are the information security requirements to supply to export markets?.....	15

How to use this booklet

This booklet was created by the Centre for Defence Industry Capability (CDIC) to assist SMEs in better navigating the standards, certifications, accreditations and compliance landscape in the defence sector.

The CDIC is an Australian Government initiative that works with industry and the Department of Defence to build a world-class, globally competitive and sustainable Australian industry.

Contact the CDIC for more tailored advice on any qualification and whether it is appropriate for your business at cdic@business.gov.au or call us on 13 28 46 or visit our website at www.business.gov.au/cdic.

Understanding general business qualifications and requirements

Do you have the required Occupational Health and Safety systems in place?

AS/NZS 4801 Occupational health and safety management systems – Requirements with guidance for use

The adoption of an occupational health and safety (OHS) management system is a legal requirement for all Australian businesses which helps safeguard the health and safety of all employees. Businesses should have effective occupational health and safety policies and objectives implemented through the establishment and ongoing assessment and review of OHS procedures.

There are two current standards that provide an occupational health and safety management framework for workplace safety to benefit employees and to reduce risks in the workplace. AS/NZS 4801 remains a current Australian Standard and is cited in a range of Australian legislation. AS/NZS ISO 45001 is an International Standard adopted in Australia as a voluntary standard. It can be used by any business regardless of size or field of activity.

A database of accredited certification bodies and companies is maintained by JAS-ANZ www.jas-anz.org.

More information is available at Standards Australia.

Do you need to consider environmental management?

ISO 14001 Environmental Management Systems

There are a range of statutory and regulatory requirements for environmental management in Australia. ISO 14001 provides a framework for an environmental management system to protect the environment and respond to the changing environmental conditions that may impact organisations.

ISO 14001 helps organisations to improve their environmental performance through more efficient use of resources and reduction of waste. This standard will enable a business to demonstrate its compliance with statutory and regulatory requirements.

ISO 14001 can be used by any business regardless of size or field of activity and is recognised internationally. A database of accredited certification bodies and companies is maintained by JAS-ANZ www.jas-anz.org.

More information is available at the [International Organization for Standardization \(ISO\)](http://International Organization for Standardization (ISO)).

Do you have a risk management plan?

ISO 31000 Risk Management

Managing risk is a critical element of business success.

ISO 31000 provides a framework that companies can refer to in order to manage risk within their organisation. Using ISO 31000 can help organisations increase the likelihood of achieving objectives,

improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

ISO 31000 can be used by any business, regardless of size or field of activity and this standard is recognised internationally. It cannot be used for certification purposes, although it does provide guidance for internal and external audit programmes.

More information is available at the [International Organization for Standardization \(ISO\)](#).

How do you manage collaborative business relationships?

ISO 44001 Collaborative Business Relationship Management Systems – Requirements and Framework

Effective collaboration requires two or more parties to engage with a shared understanding of roles and objectives.

ISO 44001 provides a framework for the effective identification, development and management of collaborative business relationships within or between organisations.

ISO 44001 can be applied on several different levels:

- a single application to an operating unit or project
- an individual relationship such as a partnership or joint venture
- multiple identified relationships such as networks and end-to-end supply chains; and
- organisation wide for all identified relationship types

ISO 44001 is applicable to private and public organisations of all sizes and is recognised internationally.

More information is available at the [International Organization for Standardization \(ISO\)](#).

Are you pro-actively managing your assets?

ISO 55001 Asset Management – Management Systems - Requirements

Asset management provides a systematic approach to the governance and realization of value from your business assets over their whole life cycles.

ISO 55001 provides a framework for the implementation and maintenance of a management system for asset management, encouraging businesses to pro-actively manage the lifecycle of their assets and helping manage the risks and costs associated with owning assets.

ISO 55001 can be used by any organisation regardless of business size and field of activity. The organisation determines to which of its assets the standard applies. A database of accredited certification bodies and companies is maintained by JAS-ANZ www.jas-anz.org.

More information is available at the [International Organization for Standardization \(ISO\)](#).

Does your quality management system meet requirements to do business in the defence industry?

What is the key quality management system required to work in the defence industry?

A quality management system compliant with ISO 9001 or AS/EN 9100 is usually a mandatory requirement for doing business with Defence and with any major manufacturers or suppliers.

The adoption of a quality management system can help to improve an organisation's overall performance and provide a sound basis for sustainable development initiatives. Such initiatives can lead to an enhanced ability to consistently supply goods and services that meet customer and compliance requirements as well as address key risks and opportunities found in a business's context and objectives.

ISO 9001 - Quality Management Systems

ISO 9001 is the recognised international standard for the development of a quality management system. It is based on a number of quality management principles including customer focus, accountability for management, approach to process and continuous improvement.

ISO 9001 can be used by any business regardless of its size or field of activity and is recognised internationally. A database of accredited certification bodies and certified companies is maintained by JAS-ANZ www.jas-anz.org.

More information is available at the [International Organization for Standardization \(ISO\)](http://www.iso.org).

AS/EN 9100D – Quality Management Systems – Requirements for Aviation, Space and Defence Organizations

AS/EN 9100D encompasses ISO 9001 and specifies additional aviation, space and defence industry requirements. AS/EN 9100 Rev D requires organisations to install a quality management system that details policies, processes, documented procedures and records that define how the company will operate, including risk management, change management, obsolescence and product safety procedures. A database of certified aerospace suppliers and certification bodies is maintained by the International Aerospace Quality Group at www.iaqg.org.

AS/EN 9100D can be used by any business operating in the aerospace sector.

More information is available at [SAE International](http://www.sae.org).

What other specific quality requirements might you need to consider?

There are a range of other situation-specific quality system requirements for the defence industry.

ISO 17025 Testing and Calibration Laboratories

ISO 17025 enables laboratories to demonstrate that they operate competently and generate valid results, promoting confidence in their work.

ISO 17025 consists of a preliminary assessment and an accreditation assessment. The preliminary assessment gives the accreditation body an opportunity to identify any weaknesses that may exist in the laboratory management system. The accreditation assessment is a comprehensive inspection of all aspects of the laboratory environment. Any deficiencies will be recorded on a non-conformance report.

ISO 17025 can be used by any business that performs testing, sampling or calibration and wants reliable results, and is recognised internationally.

More information is available at the [International Organization for Standardization \(ISO\)](#).

National Association of Testing Authorities, Australia

The National Association of Testing Authorities (NATA) is Australia's national accreditation body for the accreditation of laboratories, inspection bodies, calibration services, producers of certified reference materials and proficiency testing scheme providers throughout NATA provides independent assurance of technical competence and integrity of organisations offering testing, inspection and calibration services (collectively known as conformity assessment) for customers who require confidence in the delivery of their products and services.

Applications for accreditation with NATA can be made by any legally identifiable organisation providing testing, inspection, examination, calibration or related services.

More information is available at [NATA and the National Measurement Institute](#).

DIN 2303 Welding and allied processes – Quality requirements for production and maintenance companies for military products

DIN 2303 certification specifies the requirements for welded products for military vehicles. It is a pre-requisite to supply to key some military vehicle projects in Australia and internationally.

The DIN 2303 certification process includes employee qualifications, welding equipment, welding quality and related areas.

More information is available at [DIN](#).

ISO 3834 Quality Requirements for Fusion Welding of Metallic Materials

The adoption of a quality management system in international welding can help to improve an organisation's overall performance and qualify for some military projects.

ISO 3834 provides criteria for quality requirements for fusion welding of metallic materials, both in workshops and at field installation sites.

ISO 3834 can be used by any manufacturing-related business.

More information is available at the [International Organization for Standardization \(ISO\)](#).

ISO/IEC/IEEE 12207 Systems and Software Engineering: Software Life Cycle Processes

ISO/IEC/IEE 12207 establishes a framework for software life cycle processes that can be referenced by the software industry. This standard provides processes that can be employed for defining, controlling, and improving software life cycle processes within an organisation. It specifies processes and tasks to be applied during the acquisition of a software product or service and during the supply, development, operation, maintenance and disposal of software products.

This standard is relevant to companies wanting to instil best practices in software engineering within their company.

More information is available at the [International Organization for Standardization \(ISO\)](#).

ISO/IEC/IEEE 15288 Systems and Software Engineering: System Life Cycle Processes

ISO/IEC/IEEE 15288 establishes a common framework of process descriptions to describe the life cycle of systems created by humans. It specifies a range of parameters that are important for the effective management of any system across its life cycle. These include process controls, defined attributes and expected outcomes, and established criteria for reviews, with the ultimate goal of achieving customer satisfaction.

This standard is relevant to companies wanting to instil best practices in systems engineering within their company.

More information is available at the [International Organization for Standardization \(ISO\)](#).

ANSI Accredited ISO 17024 Conformity Assessment

Personnel certification verifies that an individual possesses the skills and knowledge required for a specific field of endeavour.

If you are running any personnel certification programs, you can seek ANSI accreditation under *ANSI/ISO/IEC 17024 Conformity Assessment – General requirement for bodies operating certification of persons*.

ANSI Accredited ISO 17024 is a certification against an international standard for the operation of personnel certification programs. It is relevant to all businesses operating personnel certification programs, and can be used by any business regardless of size or field of activity.

ANSI Accredited ISO 17024 certification demonstrates that personnel certification programs meet general requirements such as operating in a consistent, comparable and reliable manner.

More information is available at [ANSI](#).

Are you working in the aerospace industry?

There are additional specific quality and compliance requirements for businesses working in the aerospace industry.

Do you need to implement additional aerospace specific quality management?

AS/EN 9110 Quality Maintenance Systems – Aerospace – Requirements for Maintenance Organizations

AS/EN 9110 encompasses ISO 9001 and specifies additional requirements for a quality management system for aerospace maintenance organisations, including requirements critical to the maintenance of all commercial, private and military aircrafts.

AS/EN 9110 applies to all aerospace maintenance businesses.

More information is available at [SAE International](#).

AS/EN 9120 Quality Management Systems – Aerospace Requirements for Stockist Distributors

AS/EN 9120 encompasses ISO 9001 and specifies additional requirements for a quality management system for the aerospace industry applicable to stockist distributors, requiring aerospace stockists to implement a specialised quality management system.

AS/EN 9120 can be used by any business that is supplying goods and services in the aerospace sector, and applies to distributors and suppliers working with original equipment manufacturers.

More information is available at [SAE International](#).

What are the compliance requirements for the aerospace industry in key markets?

Australia: Civil Aviation Safety Authority and Defence Aviation Safety Authority

The Civil Aviation Safety Authority (CASA) and Defence Aviation Safety Authority (DASA) are Australian authorities responsible for regulating the entire aerospace supply chain. Compliance with CASA and DASA regulations is critical for any Australian business operating in the domestic aerospace industry.

CASA and DASA regulation is publically available and includes a comprehensive set of requirements that guide activities within the aerospace sector.

More information is available at [Civil Aviation Safety Authority](#) and [Defence Aviation Safety Authority](#).

United Kingdom: Civil Aviation Authority and Military Aviation Authority

The Civil Aviation Authority (CAA) and Military Aviation Authority (MAA) are the authorities responsible for regulating the entire aerospace supply chain in the United Kingdom. Compliance with CAA and MAA regulations is critical for any Australian business operating in the United Kingdom aerospace industry.

CAA and MAA regulations are publically available and include a comprehensive set of requirements that guide activities within the aerospace sector.

More information is available at [Civil Aviation Authority](#) and [Military Aviation Authority](#).

European Union: European Union Aviation Safety Agency

The European Union Aviation Safety Agency (EASA) is the main aviation authority responsible for the regulations covering the aerospace supply chain within the European Union. Compliance with EASA requirements enable businesses to supply to European aerospace markets.

EASA regulations are publically available and include a comprehensive set of regulations that guide activities within the aerospace sector.

More information is available at [European Union Aviation Safety Agency](#).

United States of America: Federal Aviation Administration and Department of Defence

The Federal Aviation Administration (FAA) and Department of Defense (DoD) are the main aviation authorities based in the US. Compliance with FAA and DoD requirements is critical for Australian businesses seeking to supply goods and services to the US aerospace and defence market.

FAA and DOD regulations are publically available and include a comprehensive set of regulations that guide activities within the defence and aerospace sector.

More information is available at [Federal Aviation Administration](#) and Department of Defence.

Canada: Transport Canada Civil Aviation and the Aerospace Authority

The Transport Canada Civil Aviation (TCCA) and the Aerospace Authority (AA) are the main aviation authorities based in Canada. Compliance with TCCA and AA regulations is critical for Australian business seeking to operate in the Canadian aerospace industry.

TCCA and AA regulations are publically available and include a comprehensive set of regulations that guide activities within the aerospace sector.

More information is available at [Transport Canada Civil Aviation](#) and Aerospace Authority.

Understanding security requirements

What security requirements do you need to meet to supply to the defence market?

Defence Industry Security Program

The Defence Industry Security Program (DISP) ensures that Australian organisations maintain their security responsibilities and safeguards the supply chain. This is achieved through risk mitigation and assurance programs.

DISP is a pre-requisite for companies wanting to work with defence-relevant information classified Protected or above.

DISP sets out a number of governance, personnel, physical and ICT/cyber security requirements depending on the nature of the organisation's business. DISP membership provides businesses with increased opportunities to work with the Department of Defence and easier access to Defence security services.

More information is available at [Defence Security and Vetting Service](#).

Defence Security Principles Framework

The Defence Security Principles Framework (DSPF) provides principles, controls and instructions to support those working in defence environments to manage security risks, including Defence personnel, defence industry, contractors, consultants and outsourced service providers.

The DSPF is applicable to organisations that handle, store, process or have contact with defence classified information.

The Department of Defence has implemented a grandfathering arrangement to cover references made to the Defence Security Manual in existing contracts until 30 June 2019. From 1 July 2019, all Defence Security Manual references in contracts will be treated as references to the DSPF.

More information is available at [Defence Security and Vetting Service](#).

Have you assessed your information security?

Essential Eight – Information Security Management

The Australian Cyber Security Centre's Essential Eight is a prioritised list of key mitigation strategies to assist organisations to improve cyber resilience and mitigate cyber incidents caused by a range of threats.

The Essential Eight are drawn from a wider list of prioritised mitigation strategies called *Strategies to Mitigate Cyber Security Incidents*. Eight of the most effective strategies are contained in Essential Eight.

While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline,

known as the Essential Eight, makes it much harder for adversaries to compromise systems. Furthermore, implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

More information is available at [Australian Cyber Security Centre](#).

ISO 27001 – Information Security Management

ISO 27001 provides a framework for managing information security risks that may arise in an organisation. Implementing this standard enables organisations to manage the security of information assets such as financial information, intellectual property, employee details or information entrusted by third parties.

The requirements outlined in ISO 27001 do not provide specific information security controls as they will be different according to the organisation's context.

ISO 27001 can be used by any business regardless of its size or field of activity and is recognised internationally.

More information is available at the [International Organization for Standardization \(ISO\)](#).

What additional information security requirements do you need to meet to supply technology goods and services to the defence market?

Australian Government Information Security Manual

The Australian Government Information Security Manual (ISM) outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats.

The ISM is applicable to organisations that handle or work with Australian Government information classified Official or above.

The ISM sets out security controls which depend on the nature of classified information handled by your organisation. Compliance with ISM ensures best practice handling of classified information.

More information is available at [Australian Cyber Security Centre](#).

ASD Cryptographic Evaluation Program

The Australian Cyber Security Centre (ACSC) conducts cryptographic evaluations on products intended to be used by Australian and New Zealand government agencies to determine whether their security architecture and cryptographic algorithms have been implemented correctly and are strong enough for the product's intended use.

An ASD Cryptographic Evaluation is required if:

- An ICT security product is used by an Australian Government agency and relies on cryptographic functionality of PROTECTED information or higher.
- An ICT security product used by an Australian Government agency is not evaluated by the Australasian Information Security Evaluation Program and relies on cryptographic functionality of PROTECTED information or higher.

The nature of the cryptographic evaluations will be determined by the risks associated with using the ICT security product.

More information is available at [Australian Cyber Security Centre](#).

High Assurance Evaluation

The Australian Cyber Security Centre conducts high assurance evaluations which provide rigorous analysis and testing to search for any security vulnerabilities in a product or system.

All high assurance evaluations must be sponsored by an Australian or New Zealand government agency.

More information is available at [Australian Cyber Security Centre](#).

Common Criteria for Information Technology Security Evaluation

The Common Criteria for Information Technology Security Evaluation is an international certification in computer security.

The Common Criteria is an international program in which accredited laboratories test IT products against standard cyber security specifications called Protection Profiles. These profiles represent the security assurance requirements for technology classes.

Common Criteria certification is relevant for those businesses seeking to supply information technology goods and services into defence.

More information is available at [Common Criteria](#).

Do you want to join global supply chains and export defence goods?

What standards do you need to meet to supply internationally?

The Allied Quality Assurance Publications (AQAP) are standards for quality assurance systems that have been developed by NATO. The standards and associated guidance documentation can be found on the [NATO website](#).

AQAP-2110 – NATO Quality Assurance Requirements for Design, Development and Production

AQAP-2110 is a NATO quality management system for design, development and production, focusing on risk management and quality planning. The adoption of the AQAP-2110 standard is a requirement of the NATO partners as well as required by US companies.

AQAP-2110 complies with the NATO policy of recognising civil standards wherever possible by invoking the requirements of ISO 9001 *Quality Management Systems*.

AQAP-2110 can be used by any business regardless of its size or field of activity.

AQAP-2110 is available on the [NATO website](#).

AQAP-2210 – NATO Supplementary Software Requirements to AQAP-2210 or AQAP-2310

AQAP 2210 is a NATO quality management system for software systems, intended for use with AQAP-2110 or AQAP-2310 as a software specific and project oriented supplement. The adoption of the AQAP-2210 standard is a clearly stated requirement of the NATO partners as well as required by US companies.

AQAP-2210 can be used by any business regardless of its size or field of activity.

AQAP-2210 is available on the [NATO website](#).

AQAP-2310 – NATO Quality Assurance Requirements for Aviation, Space and Defence Suppliers

AQAP-2310 specifies the NATO quality management system requirements for aviation, space and defence suppliers. The adoption of the AQAP-2310 standard is a clearly stated requirement of the NATO partners as well as required by US companies.

AQAP-2310 includes the requirements of AS/EN9100 *Quality Management Systems – Requirements for Aviation, Space and Defence Organizations*.

AQAP-2310 can be used by any business size regardless of its field of activity.

AQAP-2310 is available on the [NATO website](#).

Do you want to supply to the US aerospace and defence markets?

Federal Acquisition and Defence Federal Acquisition Regulations

The Federal Acquisition Regulations (FAR) and Defence Federal Acquisition Regulations Supplement (DFARS) are the rules and policies that guide all United States government procurements.

FAR and DFAR regulations are publically available and include a comprehensive set of regulations that guide procurement processes within the defence sector. Federal government agencies and contractors to the US Government, must follow the procurement rules and policies within the FAR and DFARS.

The FAR and DFAR are relevant for those businesses seeking to supply US aerospace and defence markets.

More information is available at [acquisition.gov](https://www.acquisition.gov).

US Export Controls: EAR and ITAR

The United States controls the export, import and use of a number of inherently military items, dual commercial and military items, and nuclear equipment and material, both within its borders and extraterritorially.

The Export Administration Regulations (EAR), along with the International Traffic in Arms Regulations (ITAR), are two of the most important regulations set out by the US Federal Government to regulate the trade of defence-related material.

The EAR regulate the export of 'dual-use' items which are defined as having been designed for commercial purposes but which could have military applications.

Goods and services that are inherently military in design, purpose or use must comply with ITAR. The ITAR regulations specify that such goods and services require an authorisation when seeking to import, export, or retransfer controlled articles, or for transit of defence articles through the US.

The EAR and ITAR are separate and additional to required Australian export licences. The regulations are publically available and include a comprehensive set of regulations that guide activities within the defence and aerospace sector.

The EAR can be found at the [US Department of Commerce](https://www.dhs.gov). More information on ITAR is also available at the [Directorate of Defense Trade Controls](https://www.dhs.gov).

Joint Certification Program

The Joint Certification Program (JCP) allows US and Canadian contractors to apply for access to US Department of Defense (US) and Canadian Department of National Defence unclassified export controlled technical data and/or critical technology.

JCP certification is required by US and Canadian contractors wanting to work with unclassified technical data relating to military critical technology in the US and Canada. Applicants must be a permanent resident of either the US or Canada.

More information is available at the [Defense Logistics Agency](https://www.dhs.gov).

National Aerospace and Defence Contractors Accreditation Program

The National Aerospace and Defence Contractors Accreditation Program (Nadcap) is an industry-managed approach to establish requirements for the standardised approval of aerospace and defence suppliers.

Nadcap accreditation is applicable to organisations seeking to provide goods and services to the US aerospace and defence sector.

The Nadcap program offers the opportunity for suppliers to gain tighter controls within their special processes. It also provides the forum for a voice in the establishment of audit requirements, networking, and market recognition.

More information can be found at [Performance Review Institute](#).

What are the information security requirements to supply to export markets?

NIST Special Publication 800-171

National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171) defines a set of cybersecurity requirements that must be followed by suppliers who want to be eligible for contracts with the US Department of Defence. Implementing NIST SP800-171 is required to comply with DFARS clause 254.204-7012 '*Safeguarding Covered Defense Information and Cyber Incident Reporting*'.

NIST SP800-171 is relevant for those businesses operating within the US aerospace and defence market and are handling controlled unclassified information, such as ITAR controlled information.

NIST SP800-171 security requirements apply to all organisations that process, store, or transmit controlled unclassified information.

More information is available at the [NIST Computer Security Resource Centre](#).

UK Cyber Essentials

The Cyber Essentials is a certification authorised by the UK's National Cyber Security Centre that helps business guard against the most common cyber threats and demonstrate a commitment to cyber security.

The Cyber Essentials certificate is an important certification for any business looking to supply information technology related services to the United Kingdom.

The process commences with the suppliers completing a supplier assurance questionnaire for lodgement with the certification body. Certification will mean the business will be listed on a directory of organisations awarded Cyber Essentials.

More information is available at the [National Cyber Security Centre](#).

Def Stan 05-138 Cyber Security for Defence Suppliers

Def Stan 05-138 is a standard that specifies the five levels of cyber risk that can be assessed when entering into contract with the United Kingdom's Ministry of Defence.

Def Stan 05-138 is relevant for business contracting directly with the United Kingdom's Ministry of Defence.

Def Stan 05-138 outlines the minimum required cyber security standards depending on the cyber risk level of each contract. Compliance will enable organisations to supply directly to the UK's Ministry of Defence.

More information is available at [GOV.UK](https://www.gov.uk).