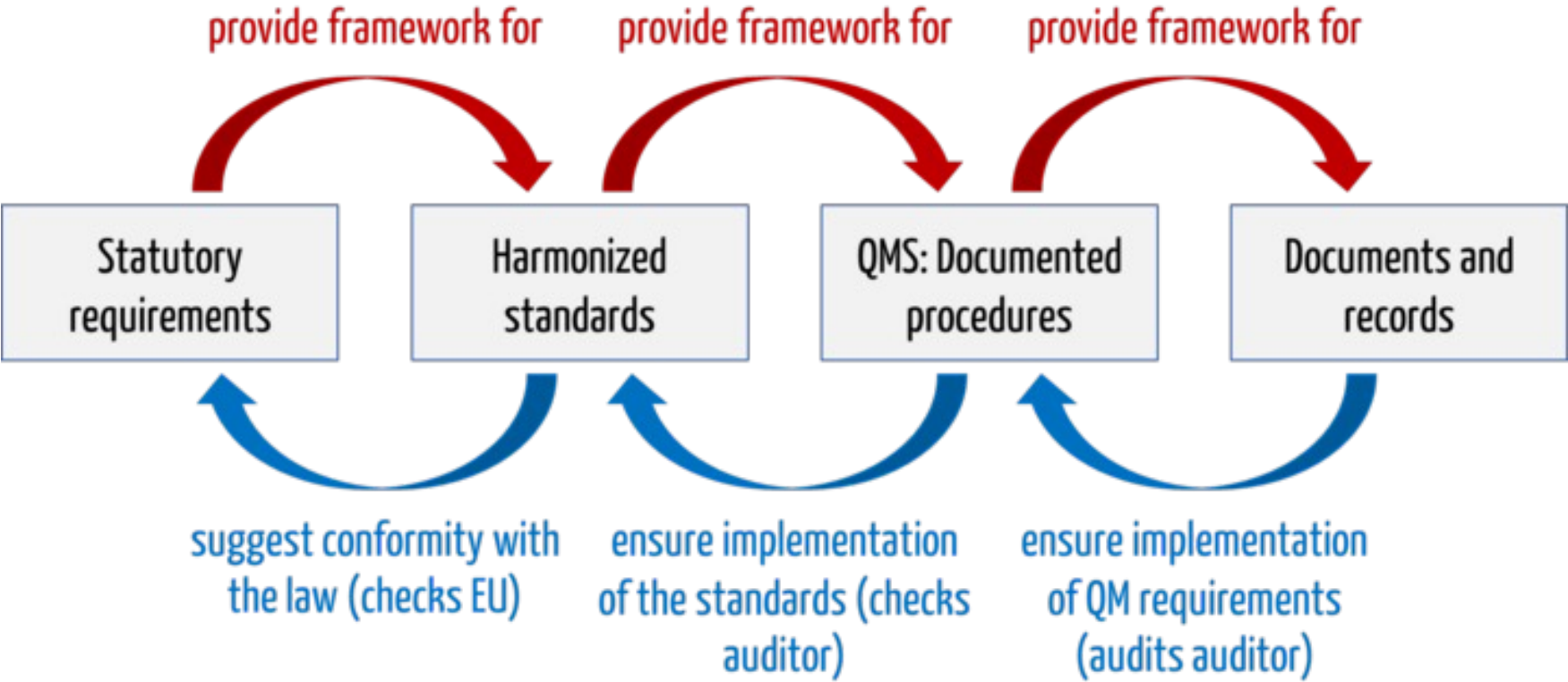


# Standards Working Together

SCSD Lecture

Thursday 29 February

# Standards and Regulation



# Harmonized Standards

- Standards compliance:
  - Is voluntary on the part of the complying organization.
  - Can be part of establishing regulatory compliance.
  - In the EU this can be particularly important as part of Harmonization across member states.
- Definition: EU Regulation 1025/2012 defines the term harmonized standard as "*a European standard adopted on the basis of a request made by the Commission for the application of Union **harmonisation** legislation.*"
- Examples
  - harmonized standards include:
    - EN IEC 62304: Software life-cycle processes for medical devices.
    - EN IEC 62366-1: Application of usability to medical devices
    - EN ISO 14971: Application of risk management to medical devices
    - EN IEC 60601-1: Medical electrical equipment and systems: Basic safety and essential performance
    - EN ISO 13485: Medical devices - Quality management systems - Requirements for regulatory purposes
- Inadequacy

## Z annexes

- These record the extent to which meeting a standard is accepted as complying with a regulation.
- For more technical standards this can be a close match.
- More procedural regulatory requirements are often more difficult to match in a standard:
  - Standards will not cover issues like registering products.
  - International standards generated by SDOs will avoid being too specific.

# Z Annexe of ISO 14971 (Risk Management, Medical Devices)

<b>General Safety and Performance Requirements of Regulation (EU) 2017/746</b>	<b>Clause(s) / subclause(s) of this EN</b>	<b>Remarks / Notes</b>
3, first paragraph	4.1 to 4.5	Covered.
3, second paragraph	4.1, 4.2	Covered.
3, item (a)	4.4	Covered in respect of the process requirements.
3, item (b)	5	Covered in respect of the process requirements. Device-specific execution of the process is not covered.
3, item (c)	5.5, 6	Covered in respect of the process requirements. Device-specific execution of the process is not covered.

# Z Annexe of ISO 13485

**Table ZB.1 – Relationship between Annex II of Directive 93/42/EEC (as amended) and the clauses of EN ISO 13485**

<b>Paragraph of Directive 93/42/EEC, Annex II</b>	<b>Clause(s) of EN ISO 13485</b>	<b>Comments/Qualifying remarks</b>
3.1 first sentence		Not covered
3.1 second sentence 1 <sup>st</sup> indent		Not covered
3.1 second sentence 2 <sup>nd</sup> indent		Not covered
3.1 second sentence 3 <sup>rd</sup> indent		Not covered
3.1 second sentence 4 <sup>th</sup> indent	4.1, 4.2	Covered provided that the documentation listed below in the comments column of this table is incorporated into the quality system documentation.

# Council Directive 93/42/EEC

## 3. Quality system

3.1. The manufacturer must lodge an application for assessment of his quality system with a notified body.

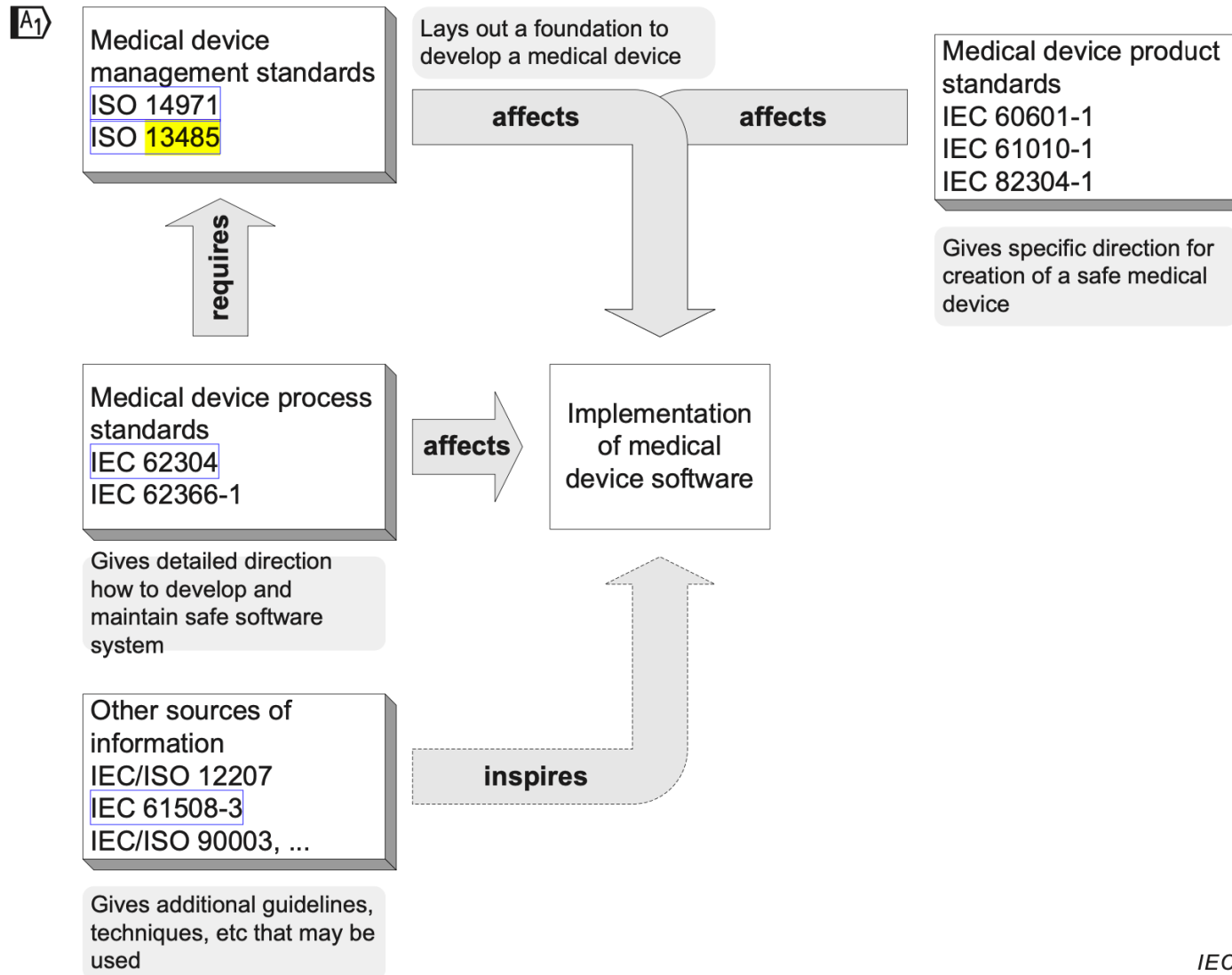
The application must include:

- the name and address of the manufacturer and any additional manufacturing site covered by the quality system,
- all the relevant information on the product or product category covered by the procedure,
- a written declaration that no application has been lodged with any other notified body for the same product-related quality system,
- the documentation on the quality system,
- an undertaking by the manufacturer to fulfil the obligations imposed by the quality system approved,
- an undertaking by the manufacturer to keep the approved quality system adequate and efficacious,
- **►M5** **↓** an undertaking by the manufacturer to institute and keep up to date a systematic procedure to review experience gained from devices in the post-production phase, including the provisions referred to in Annex X, and to implement appropriate means to apply any necessary corrective action. This undertaking must include an obligation for the manufacturer to notify the competent authorities of the following incidents immediately on learning of them: **◄**
  - - (i) any malfunction or deterioration in the characteristics and/or performance of a device, as well as any inadequacy in the instructions for use which might lead to or might have led to the death of a patient or user or to a serious deterioration in his state of health;
    - (ii) any technical or medical reason connected with the characteristics or performance of a device leading for the reasons referred to in subparagraph (i) to systematic recall of devices of the same type by the manufacturer.

# What Standards are necessary?

- **Regulation:** If the developer of a product requires regulatory compliance to a European regulator, this will often be achieved by meeting a harmonized standard.
- **International** standards reflect international consensus and this results in standards where compliance will allow considerable variation in implementation.
- **Regional:** These capture the needs of particular regions. For example, at the moment the EU is considering how best to harmonize data protection for cross-border data flows that will likely result in a harmonized standard.
- **National:** These are necessary to capture national difference. For example, there are differences in Medical Device approval between UK and EU.
- **Cross Reference:** Standards cross-refer and influence each other – most standards will list relevant other standards.





**Figure C.1 – Relationship of key MEDICAL DEVICE standards to IEC 62304**

# Deciding what standards are needed?

- For many organisations standards adoption will be considered because:
  - Standards capture good practice in the sector and demonstrating good practice can be important in mitigating product liability.
  - Standards compliance can widen access to markets e.g. compliance to harmonized standards can give access to EU markets.
  - Compliance can help expand market share. For example, compliance to sustainability standards can increase market share.
  - Standards can contribute to interoperability of interoperating products.
- Harmonization can make compliance essential to enter the market.

# Product Liability

**Since 1985, the Product Liability Directive has provided a safety net that ensures people can claim compensation when they suffer damage caused by a product.**

The new Product Liability Directive modernises the rules so they work better for emerging digital technologies, the circular economy and global value chains. Products like software, AI systems or product-related digital services are now explicitly covered by liability rules. This ensures that consumers continue to be effectively protected when products cause harm. Harmonised liability rules across the EU help to cut the cost of doing business and give businesses the certainty they need to invest in innovative products.

# Liability covers digital

## Features of the new Product Liability Directive

- ◆ The new Directive covers all products and adapts the rules to the digital age and circular economy:



Digital products are covered, including any software and AI systems.



Rules are adapted to work for new technologies, by covering cyber vulnerabilities, digital services necessary for products to function and the updates and upgrades of software and AI systems.



Products in the circular economy are covered, such as remanufactured and refurbished machinery or equipment.



# Liability arising from non-compliance



## ◆ New measures to bolster victims' rights to compensation



Consumer will be allowed to access relevant information for their claims with safeguards for confidential information.



Consumers will have a fair chance of getting compensation in complex cases and non-compliance with safety legislations (e.g. Artificial Intelligence Act (AI Act), General product safety regulation, Cyber Resilience Act and others)



Consumers will be able to get full compensation, thanks to the removal of arbitrary thresholds that limited what damage could be claimed for under the existing Directive



# Checking for omissions and consistency

- When considering a developing a product there are considerations that go beyond the immediate domain-specific standards. This may involve a considering the relevance of at least:
  - Security
  - Data Protection
  - Product liability
  - Safety
  - Sustainability
  - Accessibility
  - Equity
  - Transparency

# Constraints on systems

- Risk: DO 178C
- Engineering:
  - Interoperability: IEEE 802.11
  - Architecture: AutoSAR
  - Best practice in a domain will help define products that are recognized for quality.
    - Many products are similar to existing products.
    - This is often recognized by regulators.
    - In the USA, the FDA has a Medical Device approval route named 510k that is based on establishing a product is similar to an already approved product.

# DO178 C

## DO-178C Compliance

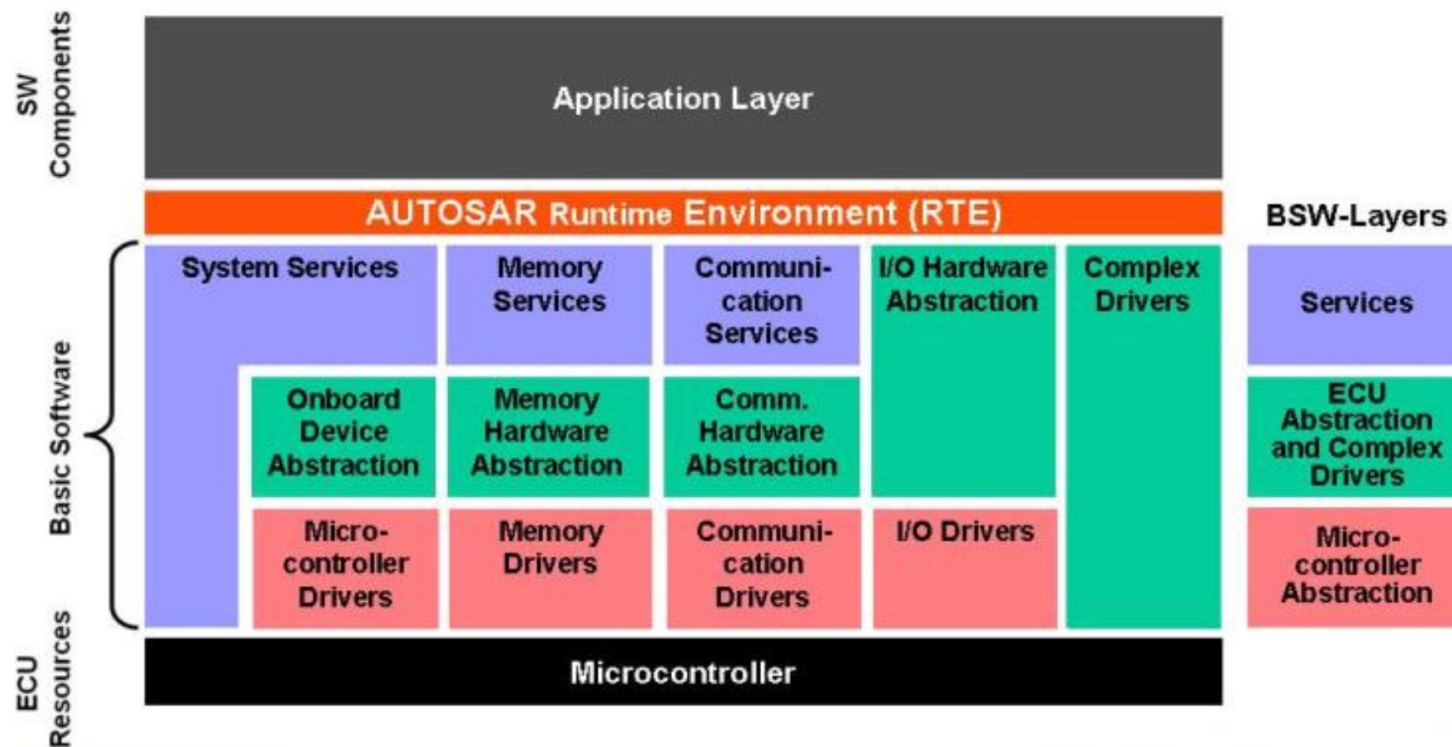
The primary objective of DO-178C is to ensure that software used in airborne systems functions as intended and does not pose any safety risks. The compliance process encompasses all aspects of software development, from planning and requirements to coding, testing, configuration management, and verification. Compliance levels, also referred to as Software Levels (DAL A, B, C, and D), are determined based on the significance of the software's function, as well as the size, complexity, and functionality of the code. The higher the DAL level, the more rigorous controls are required from software developers. And as you might expect, a DAL A system will cost a lot more time and money to produce based on the development constraints and evidence one must produce for certification.

---

<https://www.jamasoftware.com/blog/what-are-do-178c-and-ed-12c#:~:text=The%20primary%20objective%20of%20DO,%2C%20configuration%20management%2C%20and%20verification.>



# Autosar architecture



<https://gi.de/informatiklexikon/autosar-the-standardized-software-architecture>

# Product Related Constraints on Systems

- Compliance to Data Standards: DICOM, JSON, HTML, ...
- Compliance to Coding Standards: MISRA C
- Compliance to other National/Local Law e.g. Equality act.

# DICOM

## About DICOM: Overview

DICOM<sup>®</sup> — Digital Imaging and Communications in Medicine — is *the* international standard for medical images and related information. It defines the formats for medical images that can be exchanged with the data and quality necessary for clinical use.

DICOM<sup>®</sup> is implemented in almost every radiology, cardiology imaging, and radiotherapy device (X-ray, CT, MRI, ultrasound, etc.), and increasingly in devices in other medical domains such as ophthalmology and dentistry. With hundreds of thousands of medical imaging devices in use, DICOM<sup>®</sup> is one of the most widely deployed healthcare messaging Standards in the world. There are literally billions of DICOM<sup>®</sup> images currently in use for clinical care.

Since its first publication in 1993, DICOM<sup>®</sup> has revolutionized the practice of radiology, allowing the replacement of X-ray film with a fully digital workflow. Much as the Internet has become the platform for new consumer information applications, DICOM<sup>®</sup> has enabled advanced medical imaging applications that have “changed the face of clinical medicine”. From the emergency department, to cardiac stress testing, to breast cancer detection, DICOM<sup>®</sup> is the standard that makes medical imaging work — for doctors and for patients.

DICOM<sup>®</sup> is recognized by the International Organization for Standardization as the ISO 12052 standard.

<https://www.dicomstandard.org/about>

# DICOM Conformance

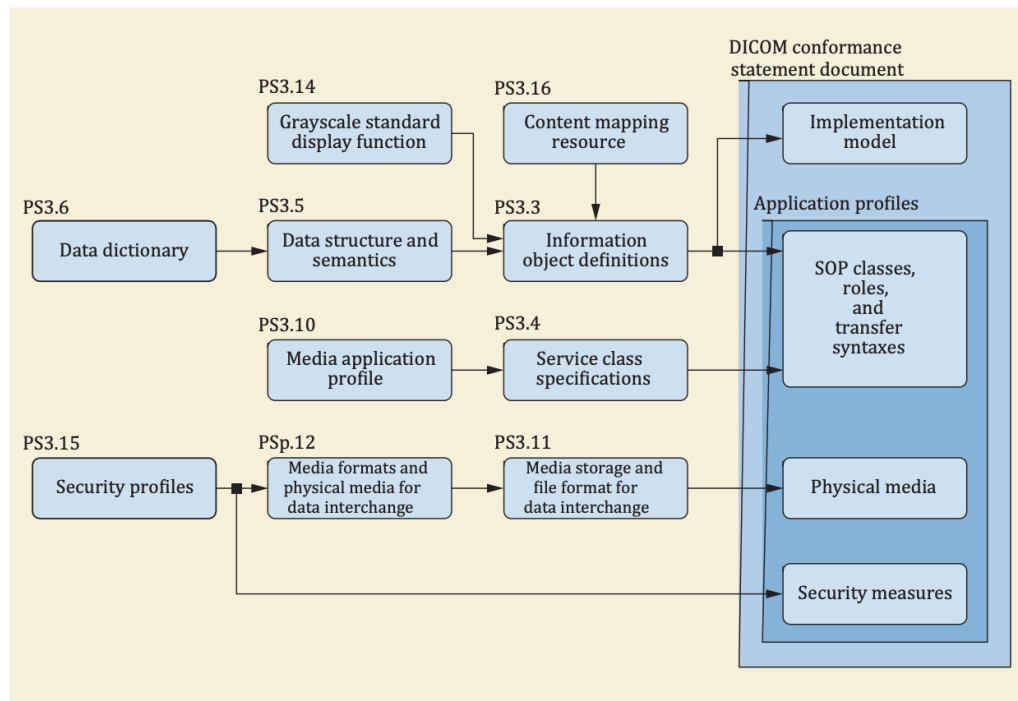


Figure 2 — Construction process for a media conformance claim

# Typical MISRA-C constraint

Rule 13.3 *A full expression* containing an increment (++) or decrement (--) operator should have no other potential *side effects* other than that caused by the increment or decrement operator

C90 [Unspecified 7, 8; Undefined 18]  
C99 [Unspecified 15; Undefined 32]  
C11 [Unspecified 16; Undefined 35]

**Category** Advisory

**Analysis** Decidable, Single Translation Unit

**Applies to** C90, C99, C11

# Process Related constraints on systems

- Specific roles and responsibilities: AI roles described in ISO 42001
- Lifecycle stages: ISO 15288: Systems and software engineering — System life cycle processes
- Process standards
  - Risk Management: ISO 14971 for medical devices
  - Quality Management: ISO 13485 for medical devices

# BS ISO/IEC/IEEE 15288

## **4.2.2 Full conformance to tasks**

A claim of full conformance declares the set of processes for which conformance is claimed. Full conformance to tasks is achieved by demonstrating that all of the requirements of the activities and tasks of the declared set of processes have been achieved. In this situation, the provisions for the outcomes of the declared set of processes are guidance rather than requirements, regardless of the verb form that is used in the provision.

**NOTE** A claim of full conformance to tasks can be appropriate in contractual situations where an acquirer or a regulator requires detailed understanding of the suppliers' processes.

# BS ISO/IEC/IEEE 15288

System Life Cycle Processes		
<b>Agreement Processes</b>	<b>Technical Management Processes</b>	<b>Technical Processes</b>
Acquisition Process (6.1.1)	Project Planning Process (6.3.1)	Business or Mission Analysis Process (6.4.1)
Supply Process (6.1.2)	Project Assessment and Control Process (6.3.2)	Stakeholder Needs and Requirements Definition Process (6.4.2)
<b>Organizational Project-Enabling Processes</b>	Decision Management Process (6.3.3)	System Requirements Definition Process (6.4.3)
Life Cycle Model Management Process (6.2.1)	Risk Management Process (6.3.4)	System Architecture Definition Process (6.4.4)
Infrastructure Management Process (6.2.2)	Configuration Management Process (6.3.5)	Design Definition Process (6.4.5)
Portfolio Management Process (6.2.3)	Information Management Process (6.3.6)	System Analysis Process (6.4.6)
Human Resource Management Process (6.2.4)	Measurement Process (6.3.7)	Implementation Process (6.4.7)
		Integration Process (6.4.8)



# BS ISO/IEC/IEEE 15288

## **A.1 General**

This annex provides requirements for the tailoring of the processes included in this document.

NOTE 1 Tailoring is not a requirement for conformance to this document. In fact, tailoring is not permitted if a claim of "full conformance" is to be made. If a claim of "tailored conformance" is made, then this process is applied to perform the tailoring.

NOTE 2 Additional guidance for tailoring can be found in the ISO/IEC/IEEE 24748-1 and ISO/IEC/IEEE 24748-2, which provide guidelines on the application of life cycle processes.

## **A.2 Tailoring process**

### **A.2.1 Purpose**

The purpose of the tailoring process is to adapt the life cycle processes included in this document to satisfy particular circumstances or factors that:

- a) surround an organization that is employing this document in an agreement;
- b) influence a project that is required to meet an agreement in which this document is referenced;
- c) reflect the needs of an organization to supply products or services.

# Summary

- We have considered collections of standards.
- How standards are interrelated.
- How standards constrain products and processes.