1. CRD table of comments, responses and resulting text

In responding to the comments, the following terminology is applied to attest EASA's position:

(a) **Accepted** — it means that EASA agrees with the comment and any proposed change is incorporated into the text

(b) **Partially accepted** — it means that EASA either partially agrees with the comment or agrees with it but the proposed change is partially incorporated into the text

(c) **Noted** — EASA acknowledges the comment, but no change to the text is considered necessary

(d) **Not accepted** — EASA does not agree with the comment or proposed change and the text will not be changed

(General Comments)	-

comment	*7* comment by: *Luftfahrt-Bundesamt* The LBA has no comments.
response	Noted. EASA thanks the LBA for the time invested in the review of this CM and for its feedback.

comment	*16* comment by: *ATR* ATR thanks EASA for the opportunity of commenting CM-21.A/21.B-001 Issue 03 proposal. ATR has no comment on it.
response	Noted. EASA thanks ATR for the time invested in the review of this CM and for its feedback.

comment	*17* comment by: *General Aviation Manufacturers Association (GAMA)* The General Aviation Manufacturers Association (GAMA) greatly appreciate the opportunity to provide comments on the Proposal of issue 03 of Certification Memorandum: Criteria for

	the determination of the EASA level of involvement in product certification. GAMA's staff remain at the Agency's disposal at any time if there are any questions regarding any of the comments provided below.
Response	Noted. EASA thanks GAMA for the time invested in the review of this CM and for its feedback.

comment	*28* comment by: *Airbus-Regulations-SRg* Airbus - Commercial Aircraft and Helicopters - are pleased to participate in this commentary. Our experts and matter specialists have carefully reviewed the EASA proposal. Our common comments are shown allocated to the dedicated Sections of "Attachment 6b - Additional guidance for Cybersecurity." In case of any question please contact our generic e-mail address regulations.policies@airbus.com for further internal coordination. Thank you. Administrative notes for all Airbus Comments: Airbus Document Classification: not applicable Airbus Export Control Classification: Not technical
response	Noted. EASA thanks Airbus for the time invested in the review of this CM and for its feedback.

comment	*45* comment by: *FOCA Switzerland* The Federal Office of Civil Aviation (FOCA) in Switzerland would like to thank EASA for having the opportunity to comment on this proposal.
Response	Noted. EASA thanks FOCA for the time invested in the review of this CM and for its feedback.

3.3 Additional panel specific guidance	p. 4

comment	*4* comment by: *Umit YUCEKAN* I propose the following revision to fix the typo in the sentence:

	"Many disciplines are transversal and should not be considered in isolation**.** (e.g. flight test, crashworthiness, electromagnetic compatibility, cybersecurity, development assurance, software, safety assessment, OSD-MMEL, etc.)
response	Accepted. EASA thanks Mr Yucekan for the time invested in the review of this CM and for his feedback. The comment is taken into account.

Attachment 6b – Additional guidance for Cybersecurity p. 27

comment	*1* comment by: *DGAC FR (Mireille Chabroux)* In paragraph A. 2 it is written that "cybersecurity is therefore transversal to several disciplines. DGAC-FR would like to know if it should be understood that cybersecurity is limited to disciplines of the panel 6 (described in 6a) or if it is also transversal to several panels.
Response	Noted. EASA thanks Ms Chabroux from the DGAC-Fr for the time invested in the review of this CM and for her feedback. As explained below in the paragraph, the *"…the applicant is expected to assess the LOI for cybersecurity at the aircraft, system and equipment not limiting it to the avionics systems.*" . No change introduced in the text due to comment 1.

comment	*2* comment by: *DGAC FR (Mireille Chabroux)* In A.2, it is written that "for organisational reasons, the LOI for cybersecurity is defined in Attachment 6 (dedicated to avioncs systems) but the applicant is expected to assess the LOI for cybersecurity at the aircraft, system ad equipement not limiting to the avionics systems. " Is the review and acceptance of the LOI solely the responsibility of panel 6 experts on the project or is it also reviewed by other involved panels ? Souldn't each involved panel accept the LOI dedicated to cybersecurity and proposed by the applicant?
response	Not accepted EASA thanks Ms Chabroux from the DGAC-Fr for the time invested in the review of this CM and for her feedback. Panel 6 coordinates internally the review with other Panels together with the Project Certification Manager (PCM). LOI is determined and notified by the Agency through the Project Certification Manager after having coordinated with all panels.

comment	*3* comment by: *DGAC FR (Mireille Chabroux)* Paragraph E states that: "With no or limited past experience, the use of avionics DOA performance rating may not be applicable and a lower rating may apply for the cybersecurity discipline." In case there is no specific performance rating dedicated to cybersecurity should we consider at first the rating of avionics DOA ? In the end, is the performance rating for cybersecurity solely the responsibility of panel 6 or is it the lowest rating of all involved panels ?
response	Noted. EASA thanks Ms Chabroux from the DGAC-Fr for the time invested in the review of this CM and for her feedback. No change introduced in the text. The need described here is already covered by the guidance material contained in Part 21, AMC 21.B.100(a) and 21.A.15(b)(6), at §3.2.4, which states that "If *one CDI affects more panels or disciplines than the others, a conservative approach should be followed in selecting the lower performance level. As an alternative, that CDI may be assessed separately for each affected EASA panel or discipline. ."*

comment	*5* comment by: *Umit YUCEKAN* As specified in chapter 3.3 of the Memo, there are many transversal disciplines (e.g flight test, crashworthiness, electromagnetic compatibility, cybersecurity, development assurance, software, safety assessment, OSD-MMEL) that needs to be evaluated in a holistic framework. In other attachments of this Memorandum, other transversal or sub-discipline-specific guidance texts are placed/embeded within the main discipline rather than forming a new sub attachment. (e.g. other transversal subjects like HIRF, EWIS is specified under Electrical Systems in Attachment 5, or DA and SA under Attachment 12). Currently at least 3 different attachment structure exist (i.e. Attachment 5, Attachment 12 and Attachment 6b) in the Memo regarding transversal subjects. In order to maintain a consistent structural organization of the attachments, a common/similar structure could be considered for all transversal subjects.
response	Noted. EASA thanks Mr Yucekan for the time invested in the review of this CM and for his feedback. EASA acknowledges this comment but does not anticipate any revision of the CM. Current framework, the particular nature and the novelty in the introduction of the cybersecurity topic makes it deserve a particular and separate chapter.

comment	*8* comment by: *FAA, Aviation Safety* Text: "For organizational reasons, the LOI for cybersecurity is defined in Attachment 6 (dedicated to avionics systems) but the applicant is expected to assess …" Comment/Rationale or Question: In addition to the LOI for cybersecurity at the aircraft, system and equipment, the applicant should include LOI for the system integration and test of the installation where the system and equipment not limiting to the avionics systems. Proposal: Suggesting the LOI for cybersecurity to include the system integration and test of the equipment installation, regardless of avionic or non-avionics equipment.
response	Not accepted EASA thanks FAA for the time invested in the review of this CM and for its feedback. Cybersecurity aspects are already covered at aircraft level cybersecurity assessment. The cyber discipline and its CDI (similarly to other panels and disciplines) already accounts for integration and test.

comment	*9* comment by: *FAA, Aviation Safety* "New connectivity methods not widely used in aviation domain" Comment/Rationale: New connectivity methods to non-trusted services or to aircraft system networks for on-board/off-board target should be considered. Proposed Resolution: Recommend to add connectivity methods for services connecting on-board/off-board targets in aircraft system.
response	Noted. EASA thanks FAA for the time invested in the review of this CM and for its feedback. The intention of the introduced sentence is broad, and covers the specific aspects addressed in the proposal of the FAA.

comment	*10* comment by: *FAA, Aviation Safety* Addition ot the List Comment: Operational Flight Software design assurance level are associated to threat levels. Any changes to the software level should corresponding to LOI. Recommendation: Recommend to add to this list of examples "software DAL level changes for operational flight software program"

response	Not accepted. EASA thanks FAA for the time invested in the review of this CM and for its feedback. From EASA point of view, DAL is associated to the safety impact severity, to the failure conditions that need to be supported by certain item when analyzed under an SSA. The association between DAL and SAL (security assurance level) is not immediate, thus introducing such an example may bring more confusion than clarification. No change in the core of the document.

comment	*11* comment by: *FAA, Aviation Safety* D. Specific aspects of complexity; addition to the list Comment: The use of AI/ML to solve system-level problems or enhance system capabilities affecting pilot training/manual, maintenance or inspection program (i.e. ICA), and human factors evaluation related. Recommendation: Suggest adding this comment to the list for specific aspects of complexity
response	Not accepted. EASA thanks FAA for the time invested in the review of this CM and for its feedback. Human factors is already covered in another chapter of the CM, and AI/ML aspects are already covered in the text "Use of artificial intelligence in the security measures" that is included in the CM.

comment	*12* comment by: *FAA, Aviation Safety* Page 28, Section E. Specific Aspect of the performance of the Design Orbanisation, “With no or limited past experience, ..” Comment: What are specific criteria for limited past experience? Should criteria be considered successfully number(s) security projects, certification experiences, experience of DOA with other cyber security standards? Recommendation: Suggest that clarifcation be provided on what limited past experiences criteria are.
Response	Noted EASA thanks FAA for the time invested in the review of this CM and for its feedback. The note “limited past experience” is intentionally left open because it is not possible to define clearly for all applicants a single criterion. It is up to EASA judgement, depending on the DOA records of the applicant

comment	*13* comment by: *FAA, Aviation Safety* Page 28, Section G. Specific aspects related to the involvement per risk class, "Risk Class" Comment: What is different between Risk Class and Security Assurance Level (SAL) ? Recommendation: Suggest that clarification be provided for the reader
response	Not accepted. EASA thanks FAA for the time invested in the review of this CM and for its feedback. SAL definition can be found on ED-203A, §4.4. For information on risk class, please see AMC 21.B.100(a) and 21.A.15(b)(6) to the part 21. In particular, §3.5 provides with the EASA expectations per risk class. Risk class has a specific meaning in the frame of LOI as defined in point 21.B.100 and no confusion is expected.

comment	*14* comment by: *FAA, Aviation Safety* Page 28-29, Section G. Specific aspects related to the involvement per risk class; "EASA's involvement per risk class" Comment: Is EASA's LOI Low, Medium, or High based only on risk class NOT a combination of risk class, SAL, novelty, simple security architecture, complex security architecture, and DOA past securities experiences? Rationale: Section C discuss Novelty. Section D discuss complexity. Section E discuss experiences Recommendation: Suggest that clarification be provided for the reader
response	Not accepted. EASA thanks FAA for the time invested in the review of this CM and for its feedback. The CM provides additional guidance for the definition of LOI as per point 21.B.100 and related AMC, where it is explained how the involvement is defined based on the novelty, complexity, Organization Performance, criticality, risk class. EASA believes that if teh CM is read in conjunction with such information, no clarification is required.

comment	*18* comment by: *General Aviation Manufacturers Association (GAMA)* Ref. Attachment 6b, G, p.29 lines 8, 14 **RATIONALE/REASON/JUSTIFICATION**

GAMA believes that including whether the witnessing of refutation/penetration testing could be conducted both on-site and remotely would be helpful.

PROPOSED TEXT/ACTION

EASA to add *"Both in-person and remote test witnessing will be acceptable"*

response

Not accepted.

EASA thanks GAMA for the time invested in the review of this CM and for its feedback. Defining if EASA will want to witness test remotely or in person will very much depend on the nature of the project and will be determined as part of EASA LOI and it is impractical to provide with procedural guidance.

comment

19 comment by: *General Aviation Manufacturers Association (GAMA)*

Ref. Attachment 6b, G, p.28

RATIONALE/REASON/JUSTIFICATION

GAMA believes that adding clarification to facilitate how the sequence of events and planned engagement will take place would be helpful. An audit checklist would also be helpful for aligned expectations.

PROPOSED TEXT/ACTION

EASA to add *"LOI and schedule will be discussed with applicant in the initial concept review. Details of expected engagement and applicable audit checklist will be provided."*

response

Not accepted.

EASA thanks GAMA for the time invested in the review of this CM and for its feedback.

Guidance on when LOI is defined is not specific of this appendix and it is out of the scope of this CM. such guidance is provided in AMC 21.B.100(a) and 21.A.15(b)(6). The additional text in the CM provides additional details and sufficient margin to ensure that the EASA and the applicant can adapt their work and involvement depending on the project nature. Considering the specificity of each project, EASA will provide audit expectation through dedicated certification material (CAI).

comment

20 comment by: *General Aviation Manufacturers Association (GAMA)*

Ref. Attachment 6b, C, p.27

RATIONALE/REASON/JUSTIFICATION

It is not clearly understood how the upcoming concept of SAL expiry relate to aspects of complexity or aspects of novelty.

PROPOSED TEXT/ACTION

EASA to clarify the question of how the upcoming concept of SAL Expiry relate to aspects of complexity or aspects of novelty

response

Not accepted.

EASA thanks GAMA for the time invested in the review of this CM and for its feedback.

Standards and guidance material under EASA's consideration (ED-202A, ED-203 and ED-204A or even ASTM F3532-22) do not contain any guidance on SAL expiry. This aspect is not taken into account for the assessment of novelty or complexity.

comment

21 comment by: *General Aviation Manufacturers Association (GAMA)*

Ref. Attachment 6b, G, p.29 Class 4

RATIONALE/REASON/JUSTIFICATION

It is not clear whether there will be a cybersecurity expert associated with the entirety of the multi-year program or only with phases of the program.

PROPOSED TEXT/ACTION

Please add *"The LOI and engagement with the assigned EASA cyber security expert will be discussed in the initial concept review."*

response

Not accepted.

EASA thanks GAMA for the time invested in the review of this CM and for its feedback. The strategy of involvement of EASA expert through the project depends also on other factors and goes beyond the LOI definition.

comment

22 comment by: *General Aviation Manufacturers Association (GAMA)*

Ref. Attachment 6b, G, p.29 Class 4

RATIONALE/REASON/JUSTIFICATION

Addition of a section/appendix outlining exactly what is to be audited and what means will be applied is necessary for the implementation of this guidance.

PROPOSED TEXT/ACTION

EASA to add section H which contains the anticipated Cyber Security Audit checklists or example checklists for each class of engagment.

response

Not accepted.

EASA thanks GAMA for the time invested in the review of this CM and for its feedback. Cybersecurity evolves quickly, thus freezing checklist of broad applicability seems impractical and out of scope of this CM which aims to provide additional guidance applicable to all projects.

comment

23 comment by: *General Aviation Manufacturers Association (GAMA)*

Ref. Attachment 6b, E, p.28

RATIONALE/REASON/JUSTIFICATION

It is not clear what is the Avionics cyber security DOA rating plan going forward.

PROPOSED TEXT/ACTION

EASA to clarify/propose an Avionics cyber security DOA rating plan.

response

Not accepted.

EASA thanks GAMA for the time invested in the review of this CM and for its feedback. No particular aspects is expected for defining DOA performance, beyond the general approach as explained in Part 21.B.100 and associated guidance material, and what is already included in this document.

comment

24 comment by: *General Aviation Manufacturers Association (GAMA)*

Ref. Attachment 6b, A.2, p.27

RATIONALE/REASON/JUSTIFICATION

It is not clear whether table in attachment 20 is to be used in conjunction with the text in attachment 6b to determine class/LOI for cyber security.

PROPOSED TEXT/ACTION

GAMA requests clarification for determining class for projects by adding in attachment 6b *"Use the risk classification table in attachment 20 to determine LOI Class."*

response

Noted.

EASA thanks GAMA for the time invested in the review of this CM and for its feedback. The CM provides additional guidance and should be read in conjunction with point 21.B.100 and related guidance. When this is done, EASA believe that no additional clarification is needed.

comment

25 comment by: *Garmin International*

Attachment 6b, Section A.2 Page 27 of 71:

Proposed Text:

Use the following term: "Intentional Unauthorized Electronic Interaction (IUEI)".

Justification:

The term "Intentional Electronic Unauthorized Interaction (IEUI)" is inconsistent with the term in RTCA/DO-356A and EUROCAE/ED-203A.

response

Accepted.

EASA thanks Garmin International for the time invested in the review of this CM and for its feedback. For information, the term IUEI is the term that is used in Part 21, in CS23 and in CS25. The term IUEI is defined in ED 202A, ED 203A, ED 204A and ER 013A.

comment

26 comment by: *Garmin International*

Attachment 6b, Section C Page 27 of 71:

Proposed Text:

Replace "new security measures" with "Inclusion of types of measures not previously used by an organization and not defined by published standards." Replace "increase or decrease of security assurance activities" with "First use of a higher security assurance level by an organization".

Justification:

The inclusion of "new security measures" and "increase or decrease of Security Assurance ctivities" in the list of "novelty" could create a perverse incentive for organizations to avoid including desirable security improvements if doing so would trigger increased agency involvement.

response

Partially Accepted.

EASA thanks Garmin International for the time invested in the review of this CM and for its feedback. The wording proposed by EASA should be seen in the context of a TC/STC but also in the context of a major change. The “new security measures” has been improved for further clarity.

comment

27 comment by: *Garmin International*

Attachment 6b, Section D Page 28 of 71:

Proposed Text:

Add text clarifying that "work-sharing schemes" need not be complex in cases where substantially similar risk assessments, system architectures and security measures have been previously accepted and the risk assessments show that risks remain acceptable.

Justification:

The proposal states "high reliance on system suppliers to undertake the risk assessment, or as the originator of critical security measures" is to be considered complex. This does not account for the use of an integrated system using measures to protect itself that are intended to be common among multiple aircraft implementations, and not specific to a particular aircraft project or aircraft manufacturer. Declaring multiple projects "complex" that all use the same system and measures could result in undesirable overhead for all parties.

response

Not accepted.

EASA thanks Garmin International for the time invested in the review of this CM and for its feedback. EASA agrees with Garmin International that there are cases for which the same supplier integrated system will be used by several aircraft manufacturers. However, some aircraft manufacturers could implement it differently or add features which would deserve EASA scrutiny. Therefore, EASA would like to keep this example to tune its LOI accordingly in function of aircraft architecture.

comment

29 comment by: *Airbus-Regulations-SRg*

PDF page 27, Attachment 6b, C. Specific aspects of novelty, general

AIRBUS COMMENT :
The change will be always novel with criteria as they are proposed, considering that there is always either
a functional change in security measure or an assurance evolution.

Therefore, as the impact is always critical (whenever there is a security impact), then the risk class is never 1.
This comment justifies the further Airbus comments for clarification about novelty criteria.

response

Noted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. As regards to novelty, the counterexample would be the installation of a new standard for one system where cybersecurity impact is expected. If such update is done for example for obsolescence reason, none of the criteria would be impacted, and thus no novelty would be declared.

For the aspect of criticality, if the change may lead to threat conditions limited to MAJOR severity, only CS25 and CS23 level 4 aircraft would be raised to class 2 if novelty is impacted. In such case (major) Aircraft other than CS25 or CS23 level 4 would be class 1 only.

comment

30 comment by: *Airbus-Regulations-SRg*

PDF page 27, Attachment 6b, C. Specific aspects of novelty,
With regard to the wording "not exhaustive" in the first sentence of the chapter C :

AIRBUS **COMMENT:**
“Novelty” should stay at concept level and not at technology level (eg., an existing security measure
modified for a new protocol should not be considered as novel).

RATIONALE:
In order to avoid as much as possible different interpretations, Airbus has defined the term "concept", as follows:
"Concept describes the functionalities of the Security Barrier (e.g. syntactic validation, filtering, semantic validation,
proxying, authentication). A concept relies on fundamental building blocks including architecture principles related
to the equipment, software, and communications. It does not rely on a specific implementation
(e.g. COTS software such as IP tables replacing Checkpoint)."

response

Not accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. The “concept” as proposed by Airbus is internal and not common to the rest of applicants and not specified in any standards. Therefore, EASA cannot introduce this new notion in the CM.

comment

31 comment by: *Airbus-Regulations-SRg*

	PDF page 27, Attachment 6b, C. Specific aspects of novelty, w.r.t. “New connectivity methods not widely used in aviation domain” **AIRBUS PROPOSED TEXT:** It is proposed to change the text as follows : “Connectivity methods that are new to either the industry as a whole, or to the applicant, including their subcontractors, or from an EASA panel perspective” **RATIONALE:** “widely” is subjective and may be interpreted differently depending on the applicant’s or on the EASA’s specialist. The wording of AMC 21.B.100(a) section 3.3.2 would be more appropriate.
response	Accepted. EASA thanks Airbus for the time invested in the review of this CM and for its feedback. Text has been improved considering this comment.

comment	*32* comment by: *Airbus-Regulations-SRg* PDF page 27, Attachment 6b, C. Specific aspects of novelty, w.r.t. "Use of existing connectivity ***methods*** with a standard not currently used in aviation domain" **PROPOSED TEXT:** "*method*" should be detailed and clarified that it addresses a concept and not a specific technology. **RATIONALE / REASON / JUSTIFICATION for the Comment:** The choice of technology or protocol is a detail, the list should remain at security concept or architecture level. In order to avoid as much as possible different interpretations, Airbus has defined the term "concept", as follows: "Concept describes the functionalities of the Security Barrier (e.g. syntactic validation, filtering, semantic validation, proxying, authentication). A concept relies on fundamental building blocks including architecture principles related to the equipment, software, and communications. It does not rely on a specific implementation (e.g. COTS software such as IP tables replacing Checkpoint)."
response	Not accepted.

	EASA thanks Airbus for the time invested in the review of this CM and for its feedback. Refer to comment 30.

comment	*33* comment by: *Airbus-Regulations-SRg* PDF page 27, Attachment 6b, C. Specific aspects of novelty, w.r.t. bullet "New security measures (e.g., addition of signature algorithm)" (The example is at implementation level) **AIRBUS PROPOSED TEXT:** Proposal: *Addition of security measures (e.g., addition of a new signature checker, addition of an application proxy) or change of the security concept.* **RATIONALE:** In order to avoid as much as possible different interpretations, Airbus has defined the term "concept", as follows: "Concept describes the functionalities of the Security Barrier (e.g. syntactic validation, filtering, semantic validation, proxying, authentication). A concept relies on fundamental building blocks including architecture principles related to the equipment, software, and communications. It does not rely on a specific implementation (e.g. COTS software such as IP tables replacing Checkpoint)."
response	Partially accepted. EASA thanks Airbus for the time invested in the review of this CM and for its feedback. The change is accepted excluding the introduction of the security concept. Please refer to comment 30.

comment	*34* comment by: *Airbus-Regulations-SRg* PDF page 27, Attachment 6b, C. Specific aspects of novelty, w.r.t. bullet "Newly applied requirements: CS2X.1319 /GM23.2500(b)/CS-APU 90(d)/CS-E 50/CS-P.230 or corresponding cybersecurity special condition" **AIRBUS PROPOSED TEXT:** It is suggested to change the text of this bullet as follows : *New requirements for a given a/c type (regulatory amendment not in the a/c certification basis yet)*

RATIONALE:
Meaning of "newly applied" should be clarified

response

Partially accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. Airbus proposal has been used and augmented to account for the products as well (engines, APU or propeller).

comment

35 comment by: *Airbus-Regulations-SRg*

PDF page 27, Attachment 6b, C. Specific aspects of novelty
w.r.t. "First **implementation** of AMC 20-42"

AIRBUS PROPOSED TEXT:
To avoid misinterpretation of the term "implementation", alternative wording may be used e.g.:
First time usage by a Design Organization of acceptable means recommended in AMC 20-42 Airworthiness information security risk assessment.

RATIONALE / REASON / JUSTIFICATION for the Comment:
EASA address as specific aspect of novelty the "first **implementation** of AMC 20-42".
Implementation Rules to the Basic Regulation are different from CS, AMC or GM adopted by the Agency.

response

Partially accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. The wording has been improved.

comment

36 comment by: *Airbus-Regulations-SRg*

PDF page 27, Attachment 6b, C. Specific aspects of novelty
w.r.t. "Alternative means and methods of demonstrating compliance (e.g., other than AMC 20-42 or ED-203A)."

AIRBUS PROPOSED TEXT:
Please remove "ED-203A" add at the end of the sentence:
Alternative means and methods of demonstrating compliance (e.g., other than AMC 20-42)

not used by the applicant on a previous certification project

RATIONALE / REASON / JUSTIFICATION for the Comment:
If the means and methods used by applicant are alternative to AMC 20-42 but always the same over various projects,
why should they be considered as "novel"?
Moreover, ED-203A is redundant with AMC 20-42 and so it could be removed

response

Partially accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback.

The specific aspects of the project may render novel the alternative to AMC 20-42.
Reference to ED-203A is agreed to be removed.

comment

37 comment by: *Airbus-Regulations-SRg*

PDF page 27, Attachment 6b, C. Specific aspects of novelty
w.r.t.. "Increase or decrease of Security Assurance activities"

AIRBUS PROPOSED TEXT:
It is suggested to change the sentence as follows :
Increase or decrease of Security Assurance activities as compared to activities that were performed by an applicant for a previous certification project.

RATIONALE:
An increase or decrease of security assurance activity should be related to activities that were performed for a previous certification project.

response

Accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback

comment

38 comment by: *Airbus-Regulations-SRg*

PDF page 28, Attachment 6b, D. Specific aspects of complexity
w.r.t. bullet "Introduction of a complex worksharing scheme with system / equipment suppliers ... "

AIRBUS PROPOSED TEXT:
It is suggested to remove the first bullet of the listing in "Section D" completely.

RATIONALE:
The link between the complexity of a security solution and the complexity of an organization is unclear.
The complexity of an organization is DOA monitoring relevant. In addition, such consideration does not
exist for the other disciplines and creates a precedence or inconsistency.

response

Not accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. The complex worksharing may lead to several layers of oversight from the applicant thereby increasing the level of complexity. Note that this criterion is also used for P10 and P12.

comment

39 comment by: *Airbus-Regulations-SRg*

PDF page 28, Attachment 6b, D. Specific aspects of complexity, general

AIRBUS COMMENT :
Modify the text to stay “at concept level”.

RATIONALE / REASON / JUSTIFICATION for the Comment:
The list gives some examples at technology level.
Complexity should stay at concept level and not at technology level
(eg., an existing security measure modified for a new protocol should not be considered as novel).
In order to avoid as much as possible different interpretations, Airbus has defined the term "concept", as follows:
"Concept describes the functionalities of the Security Barrier (e.g. syntactic validation, filtering,
semantic validation, proxying, authentication). A concept relies on fundamental building blocks
including architecture principles related to the equipment, software, and communications.
It does not rely on a specific implementation (e.g. COTS software such as IP tables replacing Checkpoint)."

response

Not accepted

EASA thanks Airbus for the time invested in the review of this CM and for its feedback.
Please refer to comment 30.

comment

40 comment by: *Airbus-Regulations-SRg*

PDF page 28, Attachment 6b, D. Specific aspects of complexity
w.r.t. last bullet: "Complex encryption methods ..."

AIRBUS PROPOSED TEXT:
It is suggested to remove the last bullet.

RATIONALE:
Complex encryption method is a solution and should be considered as a novelty criteria and not as a complex criteria.

response

Not accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. Complex encryption method counted as novel instead of complex would merge two criteria and artificially lower the LOI.

comment

41 comment by: *Airbus-Regulations-SRg*

PDF page 28, Attachment 6b, E. Specific aspects of the performance of the Design Organisation

AIRBUS COMMENT:
Please clarify criteria which would be specific to the Panel 6b.

RATIONALE:
The added value of paragraph E is not captured because rating is specific to each Panel.
It is requested to confirm whether a specific Panel 6b will be created independent from the Panel 6a Avionics.

response

Not accepted

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. It is not intended to create a panel 6b. The attachment 6b is created to provide specific LOI guidance to the panel 6 discipline “cybersecurity”. The performance rating per panel is an average rating of all disciplines related to such panel. This rating is the starting point for the risk assessment per CDI. However, if there is no available performance feedback for a certain discipline, the applied rating might be considered “unknown”, instead of taking the average rating of the available performance feedbacks related to other disciplines.

Besides, the CM does not provide information on how performances of the DOA on the panels/disciplines are identified and this comment goes beyond the CM and text will not be changed

comment	*42* comment by: *Airbus-Regulations-SRg* PDF page 28, Attachment 6b, F. Specific aspects of criticality **AIRBUS COMMENT:** Add a sentence specifying the condition for a classification as "critical" **RATIONALE:** The paragraph should explicitly state that when a change has an adverse effect on the safety at the aircraft level, then the classification to be considered for the criticality is "Critical"
response	Accepted. EASA thanks Airbus for the time invested in the review of this CM and for its feedback. Text has been modified for further clarity.

comment	*43* comment by: *Airbus-Regulations-SRg* PDF page 28, Attachment 6b, G. Specific aspects related to the involvement per risk class w.r.t. “Class 2” **AIRBUS COMMENT:** It is suggested to create a new version of “Class 2”, limited to the involvement on PSecAC and PSecAC summary. **RATIONALE / REASON / JUSTIFICATION for the Comment:** From experience, the limitation to the sharing of PSecAC and PSecAC summary offers a good level of visibility on all the important points of the compliance demonstration. On H/C, as per CS29, the criticality would be always set to critical, leading to at least a risk class 2 (as per § 3.3 of AMC 21.B.100(a) and 21.A.15(b)(6)) . It leads to release systematically the whole package of evidence requested for Class 2 in the paragraph G ("Specific aspects related to the involvement per risk class"). Moreover, the list and nature of evidences requested for Class 2 in the paragraph G of the Attachment 6b (Additional guidance for Cybersecurity) is not consistent with those requested, for instance, in: - Attachment 6a (Additional guidance for Avionics Systems) * the review of information that summarises the main results of the compliance demonstration,

and the AFM(S), and
* the review of a small amount of compliance data (e.g. SFHA, compliance demonstration with
CRIs or AMCs and other important compliance demonstrations).
The expected number of certification meetings is likely to be limited, and there should be no
witnessing of tests, or inspections.
- Attachment 12 (Additional guidance for the Development Assurance and Safety Assessment Panel)

response

Not accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback.

The sole provision of PSecAC and PSecAS does not offer the sufficient level of information expected for risk class 2.

Indeed, for H/C the criticality would be set to “Critical” since the MAJOR repercussion is discarded. However, a DOA rating set to High would trigger a Risk class 1 and not 2.

EASA acknowledges the number of substantiations requested for Risk Class 2 and may reduce this number in the future.

comment

44 comment by: *Airbus-Regulations-SRg*

PDF page 28/29, Attachment 6b, G. Specific aspects related to the involvement per risk class w.r.t. “Class 2” & “Class 3”

AIRBUS PROPOSED TEXT:
It is proposed to change the list of evidences in accordance with the risk class as follows :

For “Class 2”: PSecAC and PSecAC summary (at system or A/C level as relevant)
Please see also comment #43.

For “Class 3”:
- Plan for Security Aspects of Certification (PSecAC)
- Aircraft or System Security Scope Definition (ASSD or SSSD)
- Aircraft or System Security Risk Assessments (ASRA or SSRA)
- Aircraft or System Security Verification (ASV, SSV)
- System Security Integrator Guidance (SSIG), only for the system which is modified
- The information that summarises the main results of the compliance demonstration related to cybersecurity activities:
such as PSecAC Summary and Security Report (including the residual open issues or identified deviations).
[please see NOTE below]

RATIONALE:
The current wording in Class 2 addressed both the aircraft and systems levels, eg. "Aircraft and System Security Scope Definition (ASSD/SSSD)".
Class 2 and Class 3 should address either the aircraft level or the system level as relevant.
NOTE:
Moving the content of "EASA proposed class 2" into new defined class 3 listing, it is suggested *to remove* the bullet
"- Aircraft Security Operator Guidance (ASOG)"
because it is not a certification document, indeed instructions for continuing airworthiness are provided in the a/c security report or the
security accomplishment summary or equivalent (eg., Maintenance Technical note).

response

Not accepted.

EASA thanks Airbus for the time invested in the review of this CM and for its feedback. ASOG is kept being consistent with ED 20XA Series. ICAs (not only cyber) are derived from the ASOG (cyber only). No action.

comment

46 comment by: *FOCA Switzerland*

Adding a new 6b panel specifically for cybersecurity may create a certain inconsistency with the other disciplines in the avionic panel. Indeed, on the one hand, it is regularly mentioned that cyber security is no different from the other disciplines in the avionic panel and, on the other hand, a new panel is created, giving special importance to this cyber security discipline. In our view, it would be useful to be more consistent and clear about intentions. Having said that, we recognize that the particularities of cybersecurity need to be addressed in an adequate way.

response

Noted.

EASA thanks FOCA for the time invested in the review of this CM and for its feedback. No new panel is created. Panel 6 will centralize cyber activities from the EASA side by using the Annex 6b. This does not contradict the fact that cyber has to be addressed transversally.

comment

47 comment by: *FOCA Switzerland*

There is the need to make sure that we can accept the following side effect of having cyber as a discipline: when experts provide a ESoS for cyber only, this impact the DOA Performances of the entire Avionics panel. The Attachment 6.b) E. "Specific aspects of the performance of the Design Organisation" (With no or limited past experience, the use of avionics DOA performance rating may not be applicable and a lower rating may apply for the cybersecurity discipline) solves only one part of the "problem", i.e. that we can consider the DO performances of cyber different than those that DOA sharepoint provides for the entire DO Avionics panel, but it does not solve the problem of the effect of the ESoS limited to cyber ,

	that affects the entire avionics panel. True, at the moment it is like any other discipline of a panel, but then, it is inconsistent to have a dedicated attachment for cyber.
response	Noted. EASA thanks FOCA for the time invested in the review of this CM and for its feedback.

comment	*48* comment by: *FOCA Switzerland* Regarding point F, we suggest the following change. CS25 and CS 23 should be treated separately. For CS 25, critical should be hazardous or catastrophic ; for CS23, critical should be only catastrophic. The proportionality between CS 25 and CS 23 would be thus given in the LOI from the different severities and between CS 23 level 4 and CS 23 lower levels , from the different reference standard (EUROCAE ED 200X vs ASTM). Criticality has a direct impact on the resulting risk class and thus is an element of foundation of the risk based approach of the LOI. To consider CRITICAL a MAJOR Failure condition (CS 25) seems totally not lined up with PNL6 and PNL10 disciplines, where critical is only HAZ and CAT and would result in having the same LOI when a FC upon IUEI is MAJOR and when it is CAT. This is not justifiable by a risk based approach. To keep in mind: if not critical, our LOI can always be high depending on the other factors (DOA performances, novelty, complexity); with the criticality we are really answering to the question: what is the effect of an un-compliance?
response	Noted. EASA thanks FOCA for the time invested in the review of this CM and for its feedback. Firstly, it is quite difficult to compare panels. P6 and P10 have for instance many more criteria for novelty and complexity which may result in the increase of EASA LOI (e.g., use of touchscreen may be classified as novel for P6 or multiple functions in the same device may be classified as complex for P10). Secondly, the aspects of criticality are considered by EASA those mainly relevant for determining the LOI because the likelihood of threats can evolve rapidly. Eventually, the risk exposure for CS23L4 and CS25 to cyber threats is considered higher by EASA as compared to any other type of product. EASA may envisage reducing its involvement in future projects, depending also on the evolution of the certification requirements, means of compliance and related guidance material.

comment	*49* comment by: *FOCA Switzerland*

	Regarding point G, risk class 2, we suggest to replace the last element by the following one. " - The review of information that summarises the main results of the compliance demonstration related to cybersecurity activities, such as PSecAC Summary and Security Report (including the residual open issues or identified deviations), and the review of a small amount of compliance data, e.g. [Plan for Security Aspects of Certification (PSecAC) and/or Aircraft and System Security Scope Definition (ASSD/SSSD) and/or Aircraft and System Security Risk Assessments (ASRA/SSRA) and/or Aircraft and System Security Verification (ASV, SSV) and/or Aircraft Security Operator Guidance (ASOG) and/or System Security Integrator Guidance (SSIG)]." The expected number of certification meetings is likely to be limited, and there should be no witnessing of tests, or inspections. The LOI for a risk class 2 is too much comparing with the risk class 2 of many other panels (PNL6, PNL10) and audit are considered only starting from a risk class 3.
response	Not accepted. EASA thanks FOCA for the time invested in the review of this CM and for its feedback. EASA may envisage reducing its involvement in future projects, see comment 48 for more explanation of the strategy used by EASA to set the LOI for cybersecurity. Besides, EASA highlights that for class 2, no test witnessing is foreseen. No action.

comment	*50* comment by: *FOCA Switzerland* Regarding point G, risk class 3, we suggest the following text. "In addition to the activities described for risk class 2, the involvement of the EASA experts may comprise: the assessment of additional key activities and compliance data elements such as the Aircraft and System Security Architecture and Measures (ASAM, SSAM), and the witnessing of the refutation/penetration testing may be conducted, and Cybersecurity audits on the whole security process at the aircraft and system level may be conducted at one or two stages of the process." The LOI for risk class 3 presents some weaknesses (eg “cysec audits” are not recalled anymore) and not consistency with the approach for other panels to start from the lower risk class and add activities.
response	Noted. EASA thanks FOCA for the time invested in the review of this CM and for its feedback. The class 3 is cumulative with class 2 and encompasses all the activities from class2. Regulation on cybersecurity is recent and justifies this discrepancy with other panels. EASA may envisage reducing its involvement in future projects, see comment 48.

comment	*51* comment by: *FOCA Switzerland* The LOI for risk class 4 is not evidently higher than for risk class 3 and this should indeed be solved. There are also some typos e.g “expert” should read “experts”.
response	Partially agreed. EASA thanks FOCA for the time invested in the review of this CM and for its feedback. Typo corrected. Besides, the class 4 offers the possibility to EASA to audit at all stages of the process. Lower risk class do not offer this possibility.

comment	*52* comment by: *ANAC* **Place**:(1) page 28, section G, description of class 2; (2) page 29, section G, description of class 3 **Comment**: there is no indication of which specifc stage of the process will be audited. Is the intent not to define the stage, and give the freedom of the choice to the auditor? Concern: depending on the process associated to the stage(s), the selected stage(s) may be not adequate. **Proposal**: Indicate the specific stage(s) to be audited and assess if it is adequate.
response	Noted. EASA thanks ANAC for the time invested in the review of this CM and for its feedback. Freedom is given to the auditor.

comment	*53* comment by: *ANAC* **Place**: Page 28, section F **Comment**: (Typo) A "." is missing at the end of the sentence "... an adverse effect on aircraft-level safety" **Proposal**: Insert character "." after the word "safety".
response	Accepted. EASA thanks ANAC for the time invested in the review of this CM and for its feedback. The sentence has been slightly modified for better understanding.

comment	*54*	comment by: ***ANAC***
	Place: page 29, section G, class 4 **Comment**: For the sake of alignment with the contents of Class 2 and Class 3, replace "audits of the security process" with "audits of the entire security process" **Proposal**: Indicate that the entire security process will be audited	
response	Not accepted. EASA thanks ANAC for the time invested in the review of this CM and for its feedback. Having mentioned “at every stage of the process” is similar to the “entire” process.	

comment	*55*	comment by: ***ANAC***
	Place: page 29, section G, class 4. **Comment**: the construction "and/or" is ambiguous, and should be replaced with a more precise one. Probably, the "or" should be removed. **Proposal**: Remove the word "or".	
response	Partially accepted. EASA thanks ANAC for the time invested in the review of this CM and for its feedback. EASA has modified the sentence for a better understanding.	

comment	*56*	comment by: ***ANAC***
	Place: page 27, section C **Comment**: In Section C, the list of examples that may be considered to be novel is described as "not exhaustive", but does not provide general criteria for deciding on the aspect of novelty. **Proposal**: Provide criteria to decide about complexity, besides examples.	
response	Not accepted. EASA thanks ANAC for the time invested in the review of this CM and for its feedback. The provision of examples is a coherent with the rest of the CM and other panels. This list may be reviewed. In addition , general criteria can be found in AMC 21.B.100(a) and 21.A.15(b)(6)	

comment	*57*	comment by: ***ANAC***
	Place: page 28, section D **Comment**: In Section D, the list of examples that may be considered to be complex is described as "not exhaustive", but does not provide general criteria for deciding on the aspect of complexity.	

	Proposal: Provide criteria to decide about complexity, besides examples.
response	Noted. EASA thanks ANAC for the time invested in the review of this CM and for its feedback. The provision of examples is a coherent with the rest of the CM and other panels. This list may be reviewed. In addition , general criteria can be found in AMC 21.B.100(a) and 21.A.15(b)(6)

Attachment 19 - Additional guidance for Propulsion p. 63

comment	*15* comment by: *FAA, Aviation Safety* Page 64, "A novel interface or interaction with other part(s) or system(s) of the aircraft" Comment: A novel interface sometimes could be an aircraft system connection to/from a services or networks. Should a novel interface also be included the intra/ inter services or networks of a part connectivity to aircraft systems? Recommendation: Add novel services or networks connectivity that enables article/part connects to aircraft systems, similar denotation below: A novel interface, service of networks connection, or interaction with other part(s) or system(s) of the aircraft
response	Noted. EASA thanks FAA safety for the time invested in the review of this CM and for its feedback. This point is covered by the general statement in section 3.3 of the CM where it is mentioned that cybersecurity is a transversal discipline. By putting this general statement highlighting that cybersecurity should be tackled transversally in §3.3 (also reminded in A.2 of attachment 6b), it avoids EASA from quoting cyber aspect to each and every panel/discipline.

Attachment 21 - Abbreviations p. 67

comment	*6* comment by: *Umit YUCEKAN* Correction of typos by capitalizing the first letter of each of word in the long form. (e.g. AEH Airborne ~~e~~Electronic ~~h~~Hardware, DAL Design ~~a~~Assurance ~~l~~Level and similarly for the long forms of the following: HAS, HCI, IMA, NDI, PHAC, PSAC, RTO, SAS, SCI, SHM)

response	Accepted. EASA thanks Mr Yucekan for the time invested in the review of this CM and for his feedback.