|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | (EU) 2023/203, Del-IS.I.OR   *(Version 2025-09-15)* | | | |  |
|  | | | | | |
| Operatör | | | | | |
|  | | | | | |
| Organisationsnummer | | | Övrig information | | |
|  | | |  | | |
| Transportstyrelsen | | | | | |
| Ärendenummer | | Handläggare | | Berörda sektioner/samråd | |
|  | |  | |  | |
| Information | | | | | |
|  | | | | | |
| Denna checklista är avsedd att vara ett stöd för att uppnå regeluppfyllelse mot Del-IS.I.OR i Kommissionens Förordning (EU) 2023/203.  Vid diskrepanser mellan detta dokument och aktuella förordningar är det de publicerade förordningarna på EASAs hemsida som gäller.  Relevanta regelparagrafer i detta dokument följs av en ruta där operatören anger var i manualverket paragrafen omhändertagits och detta ska skrivas på detaljnivå för att underlätta och påskynda granskning och handläggning.  Checklistan är markerad enligt följande för ändringsförordning XXXX/XX eller AMC/GM (se nedan)   |  |  | | --- | --- | | Ny regelpunkt: | Regelpunkt Rubrik och text | | Samma regelpunkt men förändrad rubrik och/eller text: | Regelpunkt Rubrik kan också påverka texten |   AMC/GM  Annex II [EDD 2023/009/R] Issue 1 (Part-IS.I.OR)  Annex II [EDD 2025/014/R] Issue 1 (Part-IS.I.OR) | | | | | |
| PART-IS.I.ORANNEX II – INFORMATION SECURITY – ORGANISATION REQUIREMENTSIS.I.OR.100 Scope | | | | | |
|  | | | Ref i manualverket | | TS notering |
| IS.I.OR.100 Scope [(EU) 2023/203] | | |  | |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.200 Information security management system (ISMS) | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.200 Information security system (ISMS) [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.200 Information security management system (ISMS) + ISMS implementation and maintenance + Plan-Do-Check-Act approach + Benefits of an ISMS + Relation to ISO / IEC 27001 + Part-IS versus ISO /IEC 27001:2022 cross reference table [EDD 2025/014/R] |  |  |
| AMC1 IS.I.OR.200(a)(1) Information security management system (ISMS) [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.200(a)(1) Information security policy and objectives [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.200(a)(12) Compliance monitoring [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.200(a)(12) Compliance monitoring [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.200(a)(13) Information security management system (ISMS) [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.200(c) Information security management system (ISMS) [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.200(c) Information security management system (ISMS) [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.200(d) Proportionality in ISMS implementation + Supported implementation of the ISMS + Integration of ISMS under this regulation with existing management systems [EDD 2025/014/R] |  |  |
| AMC1 IS.I.OR.200(e) Derogation [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.200(e) Information security management system (ISMS); Application for a derogation + Evaluation of the request for a derogation + Expectations and recommendation after derogation approval + Examples [EDD 2025/014/R] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.205 Information security risk assessment | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.205 Information security risk assessment [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.205 Information security risk assessment [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.205(a) Information security risk assessment [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.205(a) Scope and boundaries indentification [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.205(b) Information security risk assessment [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.205(b) Risk information sharing + Two categories of interfacing organisations [EDD 2023/009/R] |  |  |
| GM2 IS.I.OR.205(b) Examples of aviation services *(see Appendix III)*  [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.205(c) Information security risk assessment [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.205(c) Risk assessment + Protection + Exposure reduction *(as defined in EUROCAE ED-203A)* + Attack attempt *(as defined in EUROCAE ED-203A)* + Risk acceptance criteria + Threat scenario identification + Additional methods to identify relevant threat scenarios + Examples of threat scenarios *(see Appendix I)* [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.205(d) Information security risk assessment [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.205(d) Information security risk assessment [EDD 2023/009/R] |  |  |
| GM2 IS.I.OR.205(d) Information security risk assessment [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.205(e) Safety support assessment [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.205(e) Safety support assessment [EDD 2023/009/R] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.210 Information security risk treatment | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.210 Information security risk treatment [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.210 Information security risk treatment [EDD 2025/014/R] |  |  |
| AMC1 IS.I.OR.210(a) Information security risk treatment [EDD 2023/009/R] |  |  |
| IS.I.OR.215 Information security internal reporting scheme | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.215 Information security internal reporting scheme [(EU) 2023/203] |  |  |
| AMC1 IS.I.OR.215(a) & (b) Information security internal reporting scheme  [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.215(a) & (b) Relationship between internal and external reporting  [EDD 2023/009/R] |  |  |
| GM2 IS.I.OR.215(a) & (b) Organisation of collection and evaluating of information security events [EDD 2023/009/R] |  |  |
| GM3 IS.I.OR.215(a) & (b) Relevant information for incidents and vulnerabilities [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.215(c) Information security internal reporting scheme [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.215(d) Information security internal reporting scheme [EDD 2023/009/R] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.220 Information security incidents – detection, response and recovery | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.220 Information security incidents – detection, response and recovery [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.220 Information security incidents – detection, response and recovery [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.220(a) Detection + Detection strategy [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.220(a) Detection strategy [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.220(b) Incidents + Vulnerabilities [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.220(b) Information security incidents – detection, response and recovery [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.220(b) Information security incidents – detection, response and recovery [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.220(b) & (c) Recovery objectives and timing [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.220(c) formation security incidents – detection, response and recovery [EDD 2023/009/R] |  |  |
| IS.I.OR.225 Response to findings notified by the competent authority | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.225 Response to findings notified by the competent authority  [(EU) 2023/203] |  |  |
| AMC1 IS.I.OR.225 Response to findings notified by the competent authority  [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.225 Response to findings notified by the competent authority  [EDD 2023/009/R] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.230 Information security external reporting scheme | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.230 Information security external reporting scheme [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.230 Information security external reporting scheme; Examples + Special cases [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.230(a)&(b) Information security external reporting scheme [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.230(a)&(b) Relation between IS.I.OR.230(b) and Regulation (EU) No 376/2014 + Follow-up analysis + Significant risk to aviation safety + Relation between IS.I.OR.230(b)(1) and other reporting requirements of information security occurrences related to aviation products or parts [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.230(c) Information security external reporting scheme [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.230(c) Information security external reporting scheme  [EDD 2023/009/R] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.235 Contracting of information security management activities | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.235 Contracting of information security management activities [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.235 Contracting of information security management activities [EDD 2023/009/R] |  |  |
| GM2 IS.I.OR.235 Contracting of information security management activities [EDD 2023/009/R] |  |  |
| GM3 IS.I.OR.235 Contracting of information security management activities; Examples [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.235(a) Oversight of the contracted organisation + Management of risks associated with the contracted activities [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.235(a) Prior assessment + Risk assessment associated with the provision of the contracted activities [EDD 2023/009/R] |  |  |
| GM2 IS.I.OR.235(a) Audit of contracted organisations [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.235(b) Contracting of information security management activities [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.235(b) Contracting of information security management activities [(EU) 2023/203] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.240 Personnel requirements | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.240 Personnel requirements [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.240 Personnel requirements [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.240(a)(2) Promotion of information security policy [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.240(a)(3) Basic understanding of the regulation [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(a)(3) Basic understanding of the regulation [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.240(b) Appointment of a person or group of persons  [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(b) Personnel requirements [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(b)&(c) Personnel requirements [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(c) Compliance monitoring function [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.240(d) Coordination [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(e) Common responsible person [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.240(f) Sufficient personnel [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(f) Sufficient personnel [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.240(g) Necessary competence [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(g) Necessary competence and training programme + Role-based competence framework [EDD 2025/014/R] |  |  |
| AMC1 IS.I.OR.240(h) Acknowledgement of responsibilities [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(h) Acknowledgement of responsibilities [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.240(i) Identity and trustworthiness [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.240(i) Identity and trustworthiness [EDD 2023/009/R] |  |  |
|  | | |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.245 Record-keeping | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.245 Record-keeping [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.245 Record-keeping [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.245(a)(1)(vi)&(a)(5) Record-keeping [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.245(a)(1)(vi)&(a)(5) Record-keeping [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.245(c)&(d) Record-keeping [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.245(c)&(d) Record-keeping [EDD 2023/009/R] |  |  |
| IS.I.OR.250 Information security management manual (ISMM) | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.250 Information security management manual [(EU) 2023/203] |  |  |
| GM1 IS.I.OR.250(a) Information security management manual [EDD 2023/009/R] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.255 Changes to the information security management system | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.255 Changes to the information security management system  [(EU) 2023/203] |  |  |
| AMC1 IS.I.OR.255 Changes to the information security management system  [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.255 Changes to the information security management system  [EDD 2023/009/R] |  |  |
| GM2 IS.I.OR.255 Relation between changes to the ISMS and continuous improvement + Example of changes that may have an impact on the ISMS + Example of changes that do not have an impact on the ISMS [EDD 2023/009/R] |  |  |

|  |  |  |
| --- | --- | --- |
| IS.I.OR.260 Continuous improvement | | |
|  | Ref i manualverket | TS notering |
| IS.I.OR.260 Continuous improvement [(EU) 2023/203] |  |  |
| AMC1 IS.I.OR.260 Continuous improvement [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.260 Continuous improvement [EDD 2025/014/R] |  |  |
| AMC1 IS.I.OR.260(a) ISMS effectiveness evaluation + ISMS maturity assessment [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.260(a) Continuous improvement [EDD 2023/009/R] |  |  |
| AMC1 IS.I.OR.260(b) Continuous improvement [EDD 2023/009/R] |  |  |
| GM1 IS.I.OR.260(b) Continuous improvement [EDD 2023/009/R] |  |  |

**Appendix I**

|  |  |  |
| --- | --- | --- |
| Appendix I – Examples of threat scenarios with a potential harmful impact of safety | | |
|  |  | TS notering |
| Appendix I – Examples of threat scenarios with a potential harmful impact of safety [EDD 2023/009/R] |  |  |
|  |  |  |
| Appendix IIAppendix II – Main tasks stemming from the implementation of Part-IS, mapped to the EU e-CF and NIST CSF 2.0 | | |
|  |  | TS notering |
| Appendix II – Main tasks stemming from the implementation of Part-IS, mapped to the EU e-CF and NIST CSF 2.0 [EDD 2025/014/R] |  |  |

**Appendix III**

|  |  |  |
| --- | --- | --- |
| Appendix III – Examples of aviation services and interfaces | | |
|  | Bolagets notering | TS notering |
| Appendix III – Aviation services [EDD 2025/014/R] |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | Appendix IVAppendix IV – Part-IS requirements mapping to ISA/IEC 27001:2022 clauses and controls, and considerations on differences | | | |  | Bolagets notering | TS notering | | Appendix IV – Part-IS requirements mapping ISO/IEC 27001:2022 clauses and controls, and considerations on differences [EDD 2025/014/R] |  |  |  |  | | --- | |  |   **Appendix V**   |  |  |  | | --- | --- | --- | | Appendix V – Proportionality considerations to indicators of complexity | | | |  | Bolagets notering | TS notering | | Appendix V – Proportionality considerations related to indicators of complexity [EDD 2025/014/R] |  |  |   **Appendix VI**   |  |  |  | | --- | --- | --- | | Appendix VI – Adaption of the EU Cybersecurity Skills framework (ECSF) | | | |  |  | TS notering | | Appendix VI – Adaption of the EU Cybersecurity Skills framework (ECSF)  [EDD 2025/014/R] |  |  | |

**- - - END - - -**