ILO SID Checklist

1. SID Content and Form

1.1 The SID shall be designed in a simple manner, made of durable material, with special regard to conditions at sea and be machine-readable. (C185, Article 3, paragraph 2) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.2 The issuing authority shall provide seafarers access to machines enabling them to inspect the data stored in the contactless chip. Seafarers shall be able to read all of the data stored in Data Group 1 in the LDS with appropriate captions displayed for each data field and view a displayed version of the facial image stored in Data Group 2 to verify it is a valid image of their face. (C185, Article 3, paragraph 9 and C185, Annex I, paragraph 4). ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.3 The materials used, dimensions, presentation and placement of data shall conform to the mandatory requirements for an electronic machine-readable official travel document (eMROTD), contained in Document 9303, (7th edition, 2015 or subsequent editions published by ICAO) approved by the International Civil Aviation Organization (ICAO). (C185, Annex I, paragraphs 1 and 2)

1.3.1 The physical characteristics of the SID shall be as described in Section 2 of Part 3 of ICAO Document 9303 (7th edition, 2015). (C185, Annex 1, paragraph 3) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.3.2 The dimensions of the SID shall be as described in Section 2 of Part 5 (for TD1 size SIDs) or Section 2 of Part 6 (for TD2 size SIDs) or Section 2 of Part 4 (for TD3 size SIDs) of ICAO Document 9303 (7th edition, 2015). (C185, Annex 1, paragraph 6) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.3.3 All of the information presented in the Visual Inspection Zone shall follow the requirements of Section 3 of Part 3 of ICAO Document (7th edition, 2015). (C185, Annex 1, paragraph 3)

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.3.4 All of the information presented in the Machine Readable Zone (MRZ) shall follow the requirements of Section 4 of Part 3 of Document 9303 (7th edition, 2015). (C185, Annex 1, paragraph 3)

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4 The details of the data elements to be contained in the SID and their placement within the various zones described in ICAO Document 9303 (7th Edition, 2015) are given below. No other information shall be contained in the SID. (C185, Annex 1, paragraphs 6 and 7) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.1 Issuing State. The full name of the issuing state (not its ISO 3166 abbreviation) shall be printed in Zone I with no caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.2 Document type. The three English letters “SID” shall be printed in Zone I with no caption.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.3 “Chip inside” symbol described in Section 2.3 of Part 9 of Document 9303 (7th edition, 2015). This shall be printed in Zone I with no caption.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.4 Full name of seafarer. This shall be printed as the primary identifier followed by a comma and a space and then the secondary identifier, as defined in Section 3.4 of Part 3 of Document 9303 (7th edition, 2015).
This shall be printed in Zone II with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.5 Sex of seafarer. This shall be printed as a single letter, "F" for female, "M" for male, or "X" for unspecified in Zone II with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.6 Nationality of seafarer. This shall be printed as a three-letter ISO country code in accordance with Section 5 of Part 3 of Document 9303 (7th edition, 2015). This shall be printed in Zone II with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.7 Date of birth of the seafarer. This shall be printed in the format DDbMMbYYYY where “b” is a single blank space (e.g. 12 05 1968) in Zone II with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.8 Place of birth of the seafarer. This shall be printed in Zone II with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.9 A brief description of any special physical characteristics that may assist in identification of the seafarer. If the issuing authority chooses not to record any identifying characteristics or the seafarer has no particular identifying characteristics then this field shall be filled with either the word "None", or "Aucun", or "Ninguna". The caption is at the discretion of the issuing authority but a suggested caption is "Identifying Characteristics". ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.10 Unique document number assigned to the SID by the issuing authority. This shall be no more than nine characters in length and shall be printed with a caption in Zone III for TD1 and TD2 size documents or in Zone I for TD3 size documents. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.11 Date of issue of the SID, in the format "DDbMMbYYYY", where "b" is a single blank space (e.g. 31 05 2019). This shall be printed in Zone III with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.12 Date of expiry of the SID, in the format “DDbMMbYYYY” where “b” is a single blank space (e.g. 31 05 2014). This shall be printed in Zone III with a caption.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.13 Place of issue of the SID. This shall be printed in Zone III with a caption.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.14 Signature or usual mark of the seafarer. This shall be printed in Zone IV without a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.15 Photograph of the seafarer conforming to the photo specifications in Part 3 of Document 9303 (7th edition, 2015). This shall be printed in Zone V without a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.16 Statement in the English language as follows: "This document is a seafarers' identity document for the purpose of the Seafarers' Identity Documents Convention (Revised), 2003, of the International Labour Organization. This document is a stand-alone document and not a passport." This statement may alternately be provided using an equivalent translation of this text in French or Spanish. This shall be printed in Zone VI without a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.17 Name of the issuing authority, and contact details (telephone number including country code or URL of web site or both) of the focal point under Article 4, paragraph 4 of C185. This information shall be printed in Zone VI with the following caption in English - "Issuing Authority Contact Details". An equivalent translation of the caption text in French or Spanish may alternately be used. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.18 Three-line machine-readable zone printed in Zone VII as specified in Section 4 of Part 3 of Document 9303 (7th edition, 2015), containing all the mandatory data elements specified in Section 4.2 of Part 5 (for TD1 size documents) or Section 4.2 of Part 6 (for TD2 size documents) or Section 4.2 of Part 4 (for TD3 size documents). The first two characters machine-readable zone shall be “IS” for TD1 or TD2 size documents or “PK” for TD3 size documents. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.18.1 Only a subset of characters from the OCR-B typeface (size 1, constant stroke width, and a character width spacing of 2.54 mm) may appear in the MRZ as specified in Section 4.4 of Part 3 of Document 9303 (7th edition, 2015). ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.18.2 The MRZ shall follow the position and layout requirements specified in Section 3.2.1 of Part 5 of Document 9303 (7th Edition, 2015) for TD1 size documents, in Section 3.2.1 of Part 6 of Document 9303 (7th Edition, 2015) for TD2 size document or in Section 3 of Part 4 of Document 9303 (7th Edition, 2015) for TD3 size documents. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.18.3 The contents of the MRZ shall follow the data structure specified in Section 4.2.2 of Part 5 of Document 9303 (7th Edition, 2015) for TD1 size documents, in Section 4.2.2 of Part 6 of Document 9303 (7th Edition, 2015) for TD2 size document or in Section 4.2.2 of Part 4 of Document 9303 (7th Edition, 2015) for TD3 size documents. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.19 If the SID is a TD3 size document, then it shall contain the letters "PK" as the document code. This shall be printed in Zone I with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.20 If the SID is a TD3 size document, then it shall contain the issuing State, as a three-letter International Organization for Standardization country code in accordance with Section 5 of Part 3 of Doc 9303 (7th Edition, 2015). This shall be printed in Zone I with a caption. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.4.21 If the SID is a TD3 size document, then it shall contain the name of the issuing authority. This shall be printed in Zone III, with a caption.

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.5 The SID shall be protected by at least three physical security features from the list contained in Appendix A of Part 2 of Document 9303 (7th Edition, 2015). (C185, Annex I, paragraph 4).

1.5.1 First security feature from the list in Appendix A of Part 2 of Document 9303. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.5.2 Second security feature from the list in Appendix A of Part 2 of Document 9303 (7th Edition, 2015). ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.5.3 Third security feature from the list in Appendix A of Part 2 of Document 9303 (7th Edition, 2015).

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

1.5.4 Additional optional security features.

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

2. Contactless Integrated Circuit Contained in the SID

2.1 The SID shall include a contactless integrated circuit, with a data storage capacity of at least 32 kB. (C185, Annex I, paragraph 4) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

2.2 The contactless integrated circuit shall follow all the requirements for the Logical Data Structure (LDS) in Part 10 of Document 9303 (7th Edition, 2015) but shall contain only the mandatory data elements required in that Part. (C185, Annex I, paragraph 4) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

2.3 Data stored in the LDS shall be limited to the metadata and files required for the operation of the chip and its security features, as specified in Parts 9, 10, 11 and 12 of Document 9303 (7th Edition, 2015) as well as the following data elements (C185, Annex I, paragraph 4): ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

2.3.1 In Data Group 1 of the LDS, a duplication of the machine-readable zone data, as specified in Section 6.1 of Part 10 of Document 9303 (7th Edition, 2015). ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

2.3.2 In Data Group 2 of the LDS, the biometric representation required by Article 3, paragraph 8 of C185, which shall comply with Part 9 of Document 9303 (7th Edition, 2015) for the “Primary Biometric: Facial Image” and with the encoding specified in Section 6.2 of Part 10 of Document 9303. The facial image of the seafarer shall be a copy of the image shown in the visual inspection zone (VIZ) of the SID, but compressed to a size between 15 kB and 20 kB. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

2.3.3 The Security Object (EF.SOD), as specified in Section 5.2 of Part 10 of Document 9303, that is needed to validate the integrity of data stored in the LDS using the ICAO Public Key Infrastructure (PKI) defined in Part 12 of Document 9303. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

2.4 The privacy of seafarers' data stored in the contactless integrated circuit shall be protected by a Chip Access Control mechanism as described in Part 11 of Document 9303 (C185, Annex I, paragraph 4). ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

3. Digital Signatures and Public Key Infrastructure

3.1 The SID shall include a contactless integrated circuit, with a data storage capacity of at least 32 kB, encoded and digitally signed in accordance with Parts 9, 10, 11 and 12 of Document 9303. (C185, Annex I, paragraph 4). In order to accomplish this the following elements, as an absolute minimum, need to be verified. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

3.1.1 The data in the contactless chip can be read and the digital signatures authenticated by a standard ePassport reader once it has been provided with the necessary digital security certificates. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

3.1.2 A Country Signing Certification Authority (CSCA) has been established to act as the national trust point for all SIDs and to issue all of the public key certificates (e.g. Document Signer Certificates) required for authentication of the data contained in the LDS of all SIDs issued by that nation. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

3.1.3 All of the private keys, and especially the CSCA private key, are protected to prevent against loss, theft or misuse. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

3.1.4 A system is in place to ensure that the CSCA and Document Signer private keys are periodically changed in accordance with the recommendations in Part 12 of Document 9303. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

3.1.5 A system is in place to ensure that the digital certificates required to authenticate each SID are securely distributed to all participants in the ICAO PKD and that each SID can be authenticated by an inspection system which has access to the certificates stored in the ICAO PKD. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

3.1.6 A system is in place to ensure that the CSCA established as the national trust point for all SIDs is able to produce a Certificate Revocation List (CRL) if a certificate needs to be revoked, in accordance with the requirements in Section 4.3 of Part 12 of Document 9303. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4. National Electronic Database

4.1 Each member state shall maintain a national electronic database that contains a record of each seafarers' identity document issued, suspended or withdrawn by that state. (C185, Article 4, paragraph 1) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.1.1 The database record shall be updated simultaneously with the issuance of an SID and in a prompt manner when an SID is suspended or withdrawn (C185, Annex III, Part A, Section 3(b) and 3(c)) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2 The details to be provided for each record in the electronic database shall be restricted to: (C185, Annex II) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2.1 Issuing State as written in the visual inspection zone (VIZ) of the seafarers' identity document (SID).

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2.2 Full name of seafarer as written in the visual inspection zone of the SID.

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2.3 Unique nine-character document number assigned to the SID. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2.4 Date of expiry or suspension or withdrawal of the SID, written in the format DDbMMbYYYY where "b" is a single blank space (e.g. 31 05 2019). ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2.5 Compressed facial image of the seafarer as stored in the contactless integrated circuit of the SID.

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2.6 Photograph of the seafarer as printed in the visual inspection zone of the SID.

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.2.7 Details of all inquiries made concerning the SID. As a minimum, this should include a log of the date, time, and authorization of every database query which accesses the record corresponding to each individual seafarers' identity document. This includes queries made by an agent of the issuing authority, by an agent of the focal point of the issuing member state, or by a verification authority using an online query engine to access the database directly. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.3 Appropriate restrictions shall be established to ensure that no data - in particular, photographs - are exchanged, unless a mechanism is in place to ensure that applicable data protection and privacy standards are adhered to. (Convention No. 185, Article 4, paragraph 6.) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.3.1 Relevant data protection and privacy standards that are being used in the operation of the database shall be listed and an explanation provided of the procedures in place to meet those standards. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.3.2 Database encryption or appropriate access control mechanisms shall be implemented to protect seafarer information from unauthorized persons and unintended purposes. In particular, if any information is transmitted over an external network, it shall be protected to a level at least equivalent to that obtained using SSL with user authentication through a username and password. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.3.3 Direct changes to the database shall only be possible under controlled and logged circumstances by specially authorized officials of the issuing authority.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.4 The issuing authority should draw up adequate procedures for protecting the database, including a requirement for the regular creation of back-up copies of the database, to be stored on media held in a safe location away from the premises of the issuing authority. (Convention No. 185, Annex III, Part B, Section 4.2.1)

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.5 Each member state shall designate a permanent focal point for responding to inquiries, from the immigration or other competent authorities of all Members of the Organization, concerning the authenticity and validity of the seafarers' identity document issued by its authority. Details of the permanent focal point shall be communicated to the International Labour Office, and the Office shall maintain a list which shall be communicated to all Members of the Organization. (C185, Article 4, paragraphs 4, 5 and 6) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.5.1 The focal point shall be available 24 hours per day, seven days a week through the telephone number or web site recorded on each SID issued by that member state. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.5.2 Security procedures shall be in place to ensure the legitimacy of any requests coming to the focal point so that no information about any seafarers will be released to any unauthorized parties. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.5.2.1 If the inquiries to the focal point are electronic and the responses are automated then the authentication of individual requests should use a system of usernames and passwords and/or cryptographic certificates coupled with a secure distribution mechanism to pass these usernames, passwords and/or certificates from the issuing authority to the legitimate immigration and other verification authorities of other member states that express interest in having access to the focal point. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.5.2.2 If the inquiries to the focal point involve direct human contact, then the official that receives the request at the focal point must have an approved procedure for verifying the identity and authenticity of each inquiry and must record the information used to authenticate each inquiry and the nature of the inquiry. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

4.6 A separate database to contain additional information related to the issuance process such as records of the proofing documents used, the identities and authorizations of the issuing authority agents who were involved in the various stages of the issuance process, and similar information will usually be required. This database must be either physically or logically separated from the national database so that the additional information provided in the issuance database is not available through the focal point. All security and protection measures provided for the national database, as described in Sections 4.3, and 4.4 of this checklist, shall also be provided for this issuance database. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

5. Production and delivery of blank SIDs

5.1 Processes and procedures shall be in place to ensure the necessary security for the production and delivery of blank SIDs, including the following: (C185, Annex III, Part A, Section 1) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

5.1.1 All blank SIDs are of uniform quality and meet the specifications in content and form as contained in Annex I of the Convention and detailed in Section 1 of this checklist. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

5.1.2 The materials used for production are protected and controlled.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

5.1.3 Blank SIDs are protected, controlled, identified and tracked during the production and delivery processes. In the ideal case, every blank SID should have a tracking number printed on it when it is produced by the manufacturer and these stock tracking numbers should be traced from manufacture of the blank SID to delivery of the issued SID to the seafarer.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

5.1.4 Producers have the means of properly meeting their obligations in relation to the production and delivery of blank SIDs. The security mechanisms in place at the producer must ensure that the overall protection and control of blank SIDs is maintained. The producer must have sufficient experience and expertise to provide a reasonable assurance that a supply of uniform quality blank SIDs will be available over the life of the SID issuance system. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

5.1.5 The transport of the blank SIDs from the producer to the issuing authority is secure. Even with blank stock tracking procedures in place, every effort must be taken to ensure that stock is secured during shipment. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

6. Custody, handling and accountability for blank and completed SIDs

6.1 Processes and procedures shall be in place to ensure the necessary security for the custody, handling and accountability for blank and completed SIDs, including the following: (C185, Annex III, Part A, Section 2)

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

6.1.1 The custody and handling of blank and completed SIDs is controlled by the issuing authority. Secure physical storage and appropriate tracking mechanisms must be in place to ensure that no SIDs are removed, stolen or otherwise manipulated except as part of the approved processes in place as part of the SID issuance system.

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

6.1.2 Blank, completed and voided SIDs, including those used as specimens, are protected, controlled, identified and tracked. This requires that the tracking and security mechanisms used for blank stock be extended to include all SIDs, including specimens, voided, destroyed, lost, stolen and all other forms of SID. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

6.1.3 Personnel involved with the process meet standards of reliability, trustworthiness and loyalty required by their positions and have appropriate training. Procedures must be in place to validate those personnel involved with the SID issuance process. A well defined training program for those personnel, including references to all the security standards and protocols, must be demonstrated. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

6.1.4 The division of responsibilities among authorized officials is designed to prevent the issuance of unauthorized SIDs. No single person shall be able to authorize all of the steps required to issue an SID and persons responsible for reviewing audit reports from the SID database and issuance system shall be different than those who are authorized to access the database or system. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7. Processing of applications; suspension or withdrawal of SIDs; appeal procedures

7.1 Processes and procedures are in place to ensure the necessary security for the processing of applications, the completion of the blank SIDs into personalized SIDs by the authority and unit responsible for issuing them, and the delivery of the SIDs, including: (C185, Annex III, Part A, Section 3)

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.1 Processes for verification and approval ensuring that SIDs, when first applied for and when renewed, are issued only on the basis of:

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.1.1 Applications completed with all information required by Annex I of Convention No. 185. The application may be a paper application that is scanned into an electronic system, a paper application whose fields are manually copied into an electronic system, or an electronic application directly filled in by the seafarer or by an agent of the issuing authority acting on behalf of the seafarer. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.1.2 Proof of identity of the applicant in accordance with the law and practice of the issuing State. A list of acceptable identity proofing documents must be created and agents of the issuing authority must be made familiar with this list and with how to recognize and verify the documents it contains. A record of the specific proof of identity used for each seafarer must be stored as part of the SID issuance record for that seafarer, either in paper records or preferably in an electronic database. Note that the issuance electronic database is separate from the national database described in Section 4 of this checklist, since it contains additional information related to the issuance process that is not part of the national database. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.1.3 Proof of nationality or permanent residence. A list of acceptable nationality and residence proofing documents must be created and agents of the issuing authority must be made familiar with this list and with how to recognize and verify the documents it contains. A record of the specific proof of nationality or residence used for each seafarer must be stored as part of the SID issuance record for that seafarer, either in paper records or preferably in an electronic database. Note that the issuance electronic database is separate from the national database described in Section 4 of this checklist, since it contains additional information related to the issuance process that is not part of the national database. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.1.4 Proof that the applicant is a seafarer within the meaning of Article 1 of the Convention. A list of acceptable proofing documents must be created and agents of the issuing authority must be made familiar with this list and with how to recognize and verify the documents it contains. A record of the specific proof of status as a seafarer used for each SID application must be stored as part of the SID issuance record for that seafarer, either in paper records or preferably in an electronic database. Note that the issuance electronic database is separate from the national database described in Section 4 of this checklist, since it contains additional information related to the issuance process that is not part of the national database. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.1.5 Assurance that applicants, especially those with more than one nationality or having the status of permanent residents, are not issued with more than one SID. As a minimum, this should include a check of the national database to ensure a single seafarer is not issued more than one SID by the same issuing authority as well as a signed statement from the seafarer that they do not have a currently valid SID from any other issuing authority. Ideally, issuing authorities in different member states should collaborate to allow checking against national databases to ensure that a seafarer does not have a currently valid SID from any issuing authority other than the one to which the seafarer is currently applying. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.1.6 Verification that the applicant does not constitute a risk to security, with proper respect for the fundamental rights and freedoms set out in international instruments. A list of standard security procedures should be provided to ensure that the applicant is being properly verified and that their rights are being respected. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.2 The processes ensure that:

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.2.1 The particulars of each item contained in Annex II of Convention No.185 are entered in the database simultaneously with issuance of the SID, as outlined in Section 4.1 of this checklist.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.2.2 The data, photograph, signature and biometric (the "Primary Biometric: Facial Image" defined in Part 9 of Document 9303) gathered from the applicant correspond to the applicant. This requires that an agent of the issuing authority verify this as part of the issuance process.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.2.3 The data, photograph, signature and biometric gathered from the applicant are linked to the application throughout the processing, issuance and delivery of the SID. This is typically managed by electronically linking all of the elements associated with a particular application in the issuance database.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.3 Prompt action is taken to update the database when an issued SID is suspended or withdrawn, as outlined in Section 4.1 of this checklist.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.4 An extension and/or renewal system has been established to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID and in circumstances where the SID is lost. The procedures for handling these separate situations shall be documented.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.5 The circumstances in which SIDs may be suspended or withdrawn are established in consultation with ship owners' and seafarers' organizations. The procedures around the suspension or withdrawal of SIDs shall be documented and evidence provided that consultations with the relevant ship owners' and seafarers' organizations have taken place. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

7.1.6 Effective and transparent appeal procedures are in place. These procedures must be documented and notification of these procedures provided promptly to any seafarer who has their application for an SID rejected or who has their SID suspended or withdrawn. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

8. Operation, security and maintenance of the database

8.1 Processes and procedures shall be put in place to ensure the necessary security for the operation and maintenance of the database, including the following: (C185, Annex III, Part A, Section 4) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

8.1.1 The database is secure from tampering and from unauthorized access. This includes the security procedures described in Section 4.3 of this checklist, but also that the database and its backups have adequate physical security to prevent unauthorized copies being made. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

8.1.2 Data are current, protected against loss of information and available for query at all times through the focal point. This includes the requirements of Section 4 and also that the national database shall be sufficiently robust that it is available at all times through the focal point. A system where the focal point is physically separated from the national database (perhaps due to being based in a different office from the issuing authority) and only has periodic connectivity to the national database would definitely not be acceptable. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

8.1.3 Databases are not appended, copied, linked or written to other databases; information from the database is not used for purposes other than authenticating the seafarers' identity. Other than transmitting limited information to other systems for the one time verification and approval checks described in Section 7.1.1 of this checklist and responding to queries to the focal point that may require transmission of data from the national database to a legitimate verification authority, the information from both the national database and the issuance database must not be transmitted outside the issuing authority. Access must not be permitted to either database except by authorized agents of the issuing authority for purposes related to issuance of SIDs and by the agents of the focal point when querying the national database. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

8.1.4 The individual's rights are respected, including:

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

8.1.4.1 The right to privacy in the collection, storage, handling and communication of personal data. The data protection and privacy policies referenced in Section 4.3.1 of this checklist shall be followed. The data corresponding to each individual seafarer shall only be accessed by personnel that have a legitimate need to do so in the course of their duties.

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

8.1.4.2 The right of access to data concerning him or her and to have any inaccuracies corrected in a timely manner. Every seafarer shall be given the opportunity upon request to review all of the data contained in both the national database and the issuance database that relates to themselves and their SID application and to the inquiries made about them or their SID. A process shall be documented that allows the seafarer to have any inaccuracies in their data record to be corrected in a timely manner. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

9. Quality control of procedures and periodic evaluations

9.1 Processes and procedures shall be put in place to ensure the necessary security through the quality control of procedures and periodic evaluations, including the monitoring of processes, to ensure that required performance standards are met, for: (C185, Annex III, Part A, Section 5) ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

9.1.1 Production and delivery of blank SIDs ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

9.1.2 Custody, handling and accountability for blank, voided and personalized SIDs

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

9.1.3 Processing of applications, completion of blank SIDs into personalized SIDs by the authority and unit responsible for issuance and delivery

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

9.1.4 Operation, security and maintenance of the database

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

9.2 Periodic reviews shall be carried out to ensure the reliability of the issuance system and of the procedures and their conformity with the requirements of Convention No. 185. These reviews shall include the general areas described in Section 9.1 of this checklist and shall also, as far as possible, verify conformance to all of the specific elements of Sections 1-8 of this checklist.

☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found:

9.3 Procedures shall be put in place to protect the confidentiality of information contained in reports on periodic evaluations provided by other ratifying Members. Such reports may only be distributed to personnel who have a legitimate need to access them and shall not be disclosed to the general public. ☐

Member explanation of how compliance with requirement is achieved:

Auditor explanation of how compliance was tested and results found: