No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 1 - Travel Document Issuing Authority - Organizational Structure, Internal Security and General						
1.2 Organizational Structure						
101	1.2.1	Is the Travel Document Issuing Authority (TDIA) an independent governmental organization (or section) focusing only on the issuance of travel document (and other governmental ID documents)?				
102	1.2.1	Is there only one TDIA responsible for all travel documents issued?				
103	1.2.1	Does the TDIA report to a senior executive level within the government?				
104	1.2.1	Is the TDIA supported by laws and/or regulations?				
105	1.2.1	Are these laws and/or regulations enforced?				
106	1.2.1	Do these laws and/or regulations clearly set out the mandate, responsibilities, and the limits of authority of the TDIA?				
107	1.2.1	Do these laws and/or regulations permit the TDIA to operate independently and carry out its mandate without interference?				
108	1.2.1	Is the TDIA recognized as being an essential component of country security?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
109	1.2.2	No matter the organizational structure used (decentralized/centralized), is there centralized supervision and controls in place for all aspects of the issuance process?				
If the TDIA uses partners (public or private) to carry out some of its issuance functions, please answer the following questions:						
110	1.2.3	Are all entitlement decisions made exclusively by appropriate TDIA staff members?				
111	1.2.3	Are there contracts or memorandum of understanding in place describing all rights and responsibilities or the parties involved?				
112	1.2.3	Does the TDIA perform regular risk assessments, reviews and audits of partners to ensure they have adequate on-site security and safeguards?				
113	1.2.3	Is a Threat and Risk Assessment of the partners conducted prior to engaging them to carry out any issuance functions?				
1.3 Security Framework						
114	1.3.1	Is there a TDIA security team or section that is directly responsible for developing, overseeing, and managing the security framework?				
115	1.3.1	Is this team independent of the operations chain of command?				
116	1.3.1	Does this team include specially-trained security specialists for the various aspects of security?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
117	1.3.1	Does this team make regular reports on its activities to senior management?				
118	1.3.1..1	Is there a senior manager designated at the national level (headquarters) responsible for internal security controls?				
119	1.3.1..1	Is this manager a participant in the planning and decision making levels?				
120	1.3.1..1	Is this manager independent from the operational chain of command?				
121	1.3.1..1	Is there a senior officer designated at each production site (field office) responsible for internal security controls?				
122	1.3.1..1	Are these officers independent of the operational chain of command?				
123	1.3.1..1	Are these officers functions independent of the application and document processing functions?				
124	1.3.1..2	Is there a group specialized in anti-fraud in place at the headquarters and represented in each facility?				
125	1.3.1..2	Does this group liaise with other government entities that produce breeder/primary and supporting documents?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
126	1.3.1..2	Does this group liaise with government agencies that prosecute fraud when it is found?				
127	1.3.2	Is there a security policy framework in place including a comprehensive set of detailed security policies, practices, and guidelines?				
128	1.3.2	Are the security policies, practices and guidelines available in written form?				
129	1.3.2	Does this security framework affect all aspects of TDIA operations?				
130	1.3.2	Are all such security policies and practices also fully and consistently implemented in all facilities and partner organizations that are involved with travel document issuance?				
131	1.3.2	Are the security policies, practices and guidelines communicated to all employees?				
132	1.3.2	Are the security policies, practices and guidelines easy to refer to?				
133	1.3.2	Are the security policies strictly enforced?				
134	1.3.3..1	Is security a recognized high priority of the TDIA in all of its operations and facilities?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
135	1.3.3..1	Does the security framework have strong support from senior management?				
136	1.3.3..2	Is the security framework adequately supported financially?				
137	1.3.4	Does the TDIA use any techniques to establish and maintain a strong “culture of security”?				
138	1.3.4	Is there a security awareness program in place?				
139	1.3.4	Are employees regularly trained on the security policies?				
140	1.3.4	Is the operating environment such that all staff are encouraged to make suggestions on possible improvements to security practices?				
141	1.3.5	Are staff security responsibilities considered an important part of, and included in, their performance assessments?				
142	1.3.6	Does the TDIA regularly forecast work demands and surges in applications, and plan accordingly?				
143	1.3.6	Does the TDIA have constructive plans to deal with increases in demand, excess sickness, and other work overflow situations in order to maintain operations without security compromise?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
144	1.3.6	Does the TDIA maintain a group of pre-cleared background-checked and trained part-time call-up resources to use in case of overload or other under-staffed situations?				
1.4 General Security Practices						
145	1.4.1	Does the security team, or other appointed agency, regularly carry out Threat and Risk Assessments (TRAs) on all TDIA operations, in all facilities, to ensure that security is well implemented and updated?				
146	1.4.2	Does the security team, or other appointed agency, carry out regular audits and reviews to ensure that the security policies are consistently and properly practiced across all operations and offices?				
147	1.4.2	Are some of these reviews and audits unscheduled and carried out on an ad-hoc unannounced basis?				
148	1.4.2..1	Is there a compliance process in place to ensure that needed changes identified by the audits are implemented?				
149	1.4.2..2	Are there external audits carried out regularly?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 2 - Application Processes						
2.2 Application Processes and Requirements						
201	2.2.1	Are all applications processed in a uniform and consistent manner throughout the TDIA?				
202	2.2.1	Are the same standardized application forms always used?				
203	2.2.2	Are there clear written policies and practices in place covering all aspects of the application and issuance processes for first time applicants and applications for renewal of travel documents?				
2.3 Photographs						
204	2.3	Are photos taken by a commercial photographer, trusted partners or country official?				
205	2.3	Are only photos which meet ICAO Doc 9303 specifications for photos accepted?				
206	2.3	Are there mechanisms in place to reject unacceptable photos and request new ones?				
If the TDIA accepts digitized photographs, please answer the following questions:						
207	2.3	Are digitized photos taken by trusted partners or country officials?				
208	2.3	Are digitized photos transmitted securely from the point of capture to the TDIA without an opportunity for alteration?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
2.4 Secondary Biometrics						
209	2.4	Is a secondary biometric collected as part of the issuance process?				
2.5 Treatment and Protection of Personal Information						
210	2.5	Is every application logged at first receipt and its status updated throughout the application processing chain?				
211	2.5	Are individuals involved at different stages in the application handling process identified on the status log record?				
212	2.5	Are these individuals “signed off” in some fashion when they pass the application on to the next stage?				
213	2.5	Can every document (or document copy) be accounted for at all times throughout the application process?				
214	2.5	Are ALL physical copies of ANY personal information stored in appropriate locked filing cabinets or protected rooms, except when being securely worked on?				
215	2.5	Are all computerized records protected at all times by the appropriate IT Security standards?				
216	2.5	Is it true that at NO TIME applications containing personal applicant details are stored or shared via unprotected networks or portable devices that can be removed from the travel document facilities, e.g. laptops, memory sticks, discs?				
217	2.5	Is staff restricted from “working out of office” on applications?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
218	2.5	After application processing is completed, are all application materials and personal details of the applicant carefully and securely stored in appropriately locked cabinets and protected rooms, and in appropriate IT security-protected databases?				
219	2.5	Is access to the archived records, whether manual or digitized, also subject to strict “permission” control and access logging and tracking?				
220	2.5	Are appropriate destruction or shredding devices used to destroy any information no longer required?				
221	2.5.1	Have automated passport issuing processes been implemented?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 3 - Entitlement Processes						
3.1 Summary						
301	3.1	Are all entitlement decisions made by appropriately trained TDIA staff?				
3.2 Treatment of First Applications versus Renewals						
302	3.2	Are first time applicants given special attention and treatment for identity confirmation and entitlement validation?				
303	3.2	Is the application data submitted in support of a renewal application compared to details of travel documents previously issued to that individual?				
304	3.2	Are there special reviews and scrutiny practices carried out for renewal applications submitted a long time (> two years) after expiry of the previous travel document?				
3.3 Applications for Children						
305	3.3	Are children issued their own passports?				
3.4 Documentary Evidence						
306	3.4	Are two or more trusted breeder and support documents submitted by new applicants?				
307	3.4	Are the breeder and support documents that are accepted official government documents?				
308	3.4	Where possible, are these documents required to contain specified security features and secure photos?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
309	3.4	Are there any special procedures defined for dealing with new applicants possessing limited breeder documentation, e.g. an older paper birth certificate with no photo, an older social security document, no driver's license, etc.?				
310	3.4	Are these breeder and support documents scanned and stored on the applicant's database record for renewals or future reference?				
311	3.4	Are the breeder and support documents retained by the TDIA during the application process and returned to the applicant with the travel document?				
312	3.4	Are these scanned breeder and supporting documents universally used for visual comparison purposes with the renewal application?				
313	3.4	Is the expiring or expired travel document always required for renewal applications?				
314	3.4	Is the old travel document submitted to a detailed electronic and visual comparison to its record on file?				
315	3.4	Are at least two of the physical security features of the old travel document verified forensically?				
316	3.4	If the previous travel document is an ePassport, is the chip information read and validated?				
317	3.4.1..1	Are these documents universally subject to basic forensic review?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
318	3.4.1..1	Are employees receiving applications trained to validate the authenticity of breeder and support documents?				
319	3.4.1..2	Do entitlement officers have access to comprehensive documentation, or databases, containing images and specifications of each kind of breeder or support document accepted?				
320	3.4.1..3	Are these documents regularly verified with the issuing authorities or checked through a shared connection to the databases of the breeder document issuing authorities?				
321	3.4.1..3	Are death records always checked for all applications?				
3.5 Other Means of Identifying Applicants						
322	3.5.1	Where first-time applicants are required to apply in person are they interviewed?				
323	3.5.1	Are interviews conducted where there is doubt regarding the integrity of the information and documentation provided?				
324	3.5.1	For an appearance in person or an interview are the employees receiving the application adequately trained to determine prima facie identity and application validity?				
325	3.5.1	Does this specifically include judgment of personal mannerisms and “confidence” of the applicant, similar to that carried out by trained border officials?				
326	3.5.1	During a personal appearance is the applicant compared to the photo being submitted?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
327	3.5.2	Are guarantors used for first time applications where interviews are not conducted?				
328	3.5.2	Are guarantors members of a recognized association where current address and contact information is maintained and can be verified by the TDIA?				
329	3.5.2	Are they holders of current passports (or other travel documents)?				
330	3.5.2	Are guarantors disqualified if they are paid by the applicant for acting as guarantor?				
331	3.5.2	Is there a clear policy in place against such payments and does it appear on the individual's application form signed by the guarantor?				
332	3.5.2	Are guarantors required to sign and date at least one of the photos submitted by new applicants?				
333	3.5.2	Are such guarantors disqualified if they are closely related to the applicant, e.g. siblings, parents, grandparents, children, uncles and aunts, or step and in-law relationships?				
334	3.5.2	Are guarantors contacted on a regular basis to verify their statement?				
335	3.5.2	Are guarantors contacted when there is doubt about the identity of the applicant?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
336	3.5.3	Are any personal references provided with the application?				
337	3.5.3	Are these references independent and unrelated to the applicant and each other?				
338	3.5.3	Are these references contacted to verify the identity claimed by applicants?				
339	3.5.4	Is the applicant’s social footprint verified to confirm a claimed identity?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 4 - Treatment of Materials and Blank Books						
4.1 Summary						
401	4.1	Does the TDIA have documented policies and procedures related to the treatment of materials and blank books?				
4.2 Book Production						
402	4.2	Are all materials and blank books stored in high security zones?				
403	4.2	If the travel document is produced by a third party in independent facilities, are the security levels for storage of materials and books also high?				
4.3 Numbering						
404	4.3	Are travel document blanks individually numbered such that each one can be identified at any point in the storage and issuance processes?				
405	4.3	Is the number the same as the travel document number eventually issued?				
406	4.3	Does this number appear on each interior page?				
407	4.3	Is the number printed on or laser-perforated through all interior pages?				
408	4.3	Is each internal page of each travel document numbered in sequence?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
409	4.3	Are page numbers also imprinted with UV ink?				
4.4 Shipping and Storage						
410	4.4	Are travel document blanks stored in highly secure areas, such as a vault or safe, with highly-restricted access?				
411	4.4	Is such access limited to small group of trusted individuals having supervisory authority?				
412	4.4	Is the access controlled using ID cards, biometrics, pass codes, etc.?				
413	4.4	Does this protection include 24-hour guarding of the areas or of the facility overall?				
414	4.4	Are the areas where materials and blanks are stored subject to physical security protection appropriate to the security classification of those assets (see section 7)?				
415	4.4	Does this protection include reasonable safeguards against fire and catastrophic losses?				
416	4.4	Are these storage areas backed up with alternate secure storage locations such that travel document issuance may continue in the event of catastrophic loss?				
417	4.4	Are blank books transported with the equivalent safeguards of the storage area such as by armored vehicle used to transfer cash?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
418	4.4	Do the transmitter and the receiver both have to sign off on batches received?				
419	4.4	Is the assignment of blank books to production staff carried out with a minimum of two authorized individuals (four eyes)?				
420	4.4	Are both employees required to sign for blanks stored and removed from the secure area?				
421	4.4	Are all unused books always returned to the secure area in strictly controlled time periods (such as an individual's work shift)?				
4.5 Accounting						
422	4.5	Are all books tracked, using the inventory control number, from the time they are shipped by the manufacturer to the time they are printed as a travel document or spoiled?				
423	4.5	Are blank books counted by at least two people every time they change hands?				
424	4.5	Are black books counted by at least two people when removed from the safe in the morning and unused books counted at night when returned to the safe at the end of the day or shift?				
425	4.5	Are these records inspected daily or on a shift basis by a third party?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
426	4.5	Are all staff members entrusted with blank books always checked on leaving secure areas to ensure that no blanks have been removed?				
427	4.5	If not, are these checks carried out randomly and frequently?				
4.6 Destruction						
428	4.6	Are all spoiled, defective, or excess blank books destroyed thoroughly in a process witnessed by at least two individuals with access privileges to the storage area?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 5 - Personalization and Delivery						
5.2 Personalization						
501	5.2	Is the personalization function carried out in a highly secure area with limited authorized access?				
502	5.2.1	Is the personalized travel document subject to a quality assurance review to ensure there are no mistakes?				
503	5.2.1	Is the MRZ read electronically and compared to the data page and the original application information (database and original forms)?				
504	5.2.1	For an eMRTD, is the chip read and the data (including the image) compared to the data page, the MRZ and the original application information?				
505	5.2.1	Is the Digital Signature verified?				
5.3 Delivery						
506	5.3.1	Are recipients required to pick up their travel document in person?				
507	5.3.1	Is the photo on the travel document data page (and chip in the case of an ePassport) checked against the database and the recipient on pickup?				
508	5.3.1	Is an ID document with picture checked on pickup?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
509	5.3.1	Are any questions regarding address, mother's maiden name, etc. asked at time of pickup to ensure the identity of recipient?				
510	5.3.1	Are any biometrics checked at pickup (facial recognition technology, fingerprints)?				
511	5.3.1	At the time of pickup does the applicant sign a receipt indicating that the travel document has been pickup?				
512	5.3.1	Are third parties prevented from picking up travel documents on behalf of the recipient?				
513	5.3.1	If third parties are permitted to pick up travel documents, do they have to present a signed authorization from the recipient that allows him or her to do this, as well as an ID with photo?				
514	5.3.1	Is the person picking up the travel document required to sign a receipt?				
If some personalized documents are mailed, please answer the following questions:						
515	5.3.2	Are reliable mail services used?				
516	5.3.2	Does the receipt of a travel document by the applicant or others living at the same address require a signature?				
517	5.3.2	If not, are there other means used to track whether an applicant has received his or her travel document (such as return of a code word or receipt)?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
518	5.3.2	Is delivery or pickup time monitored after release of a new travel document and are alerts issued if standard time periods are passed without receipt of such confirmation?				
519	5.3.2	Is confirmation of delivery or pickup entered into the TDIA system as a proactive indicator and recorded as the last stage of the issuance process?				
520	5.3.2	Are undelivered travel documents returned to the TDIA for verification of the address in the database as well as with the applicant?				
521	5.3.2	Are travel documents reported as undelivered handled in the same way as lost/stolen travel documents?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 6 - Document Security						
6.2 Machine Readable Travel Documents (MRTD)						
601	6.2	Does the country issue Machine Readable Passports (MRPs) in accordance with ICAO specifications Doc 9303 Part 1, Volume 1?	100%	TDs comply with ICAO specs but same design and security features have been in place for over 5 years	Medium	0%
6.3 Electronic Machine Readable Travel Documents (eMRTD)						
602	6.3	Does the country issue electronic Machine Readable Passports (eMRPs) in accordance with ICAO specifications Doc 9303 Part 1 Volume 2?	0%		Low	0%
603	6.3	If not, does the country have a plan and schedule to issue such eMRPs?	50%	Planning to introduce in 2013 but funding is not clear and limited information on how this will be achieved	Medium	25%
604	6.3	Does the country participate in the ICAO Public Key Directory (PKD)?	0%	No e-passport so not PKD member	Low	0%
6.4 ICAO Standards, Recommended Practices and Specifications						
605	6.4.1	Are all travel documents issued by the country compliant with ICAO specifications Doc 9303?	60%	Not all documents are fully compliant - eg diplomatic/official	Medium	20%
606	6.4.1	Are all travel documents designed with strong modern security features of the sort recommended in the **ICAO Informative Annex to Document 9303 Volume 1 Section III: "*Security Standards for Machine Readable Travel Documents*"?**	25%	Due to old design, documents are not as secure as they need to be	High	75%
607	6.4.2	Does the TDIA have an ongoing program to review and upgrade security features for its travel documents?	0%	Waiting for implementation of e-passport project	High	100%
608	6.4.2	Are all travel documents valid for a maximum of 10 years?	100%		Low	0%

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
609	6.4.2	Do all travel documents issued respect the one passport/one person policy?	100%		Low	0%
6.5 Types of Travel Documents						
610	6.5	Do all travel documents issued by the country include minimum security features?	75%	Minimum security features in standard passports but no features in any emergency or temporary passports	High	25%
611	6.5	Are Diplomatic and Special passports issued with the same blanks or materials (except book cover colour) as the regular passport?	100%		Low	0%
612	6.5	Do passports issued for single trip purposes (to return to the home country via a certain itinerary) include physical security features to prevent counterfeiting?	0%	Emergency passports are paper based with photo glued in and using easily forged authorising stamps	High	100%

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 7 - Facility Security						
7.2 Physical Security Policies						
701	7.2	Is there a physical security policy in place which covers all facilities and spaces used in the handling and issuance of travel documents?				
702	7.2	Are physical security standards compatible with government standards and guidelines and internationally accepted standards?				
703	7.2	Are all TDIA operations facilities, security and high security zones owned by the government?				
704	7.2	Do the facilities used by public and private partners meet physical security standards set by the TDIA?				
705	7.2	Are staff trained on physical security policies and practices?				
706	7.2	Are there sanctions for staff who do not follow the security policies and practices?				
7.3 Security Zones						
707	7.3	Are the various issuance facilities and work zones defined in terms of different security zones (Public Zone, Reception Zone, Operation Zone, Security and High Security Zones)?				
708	7.3	Are these different zones subject to different levels of physical security protection as appropriate?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
709	7.3	Do they include security practices to be followed for access control?				
710	7.3 &7.4	Do they include security practices to be followed for monitoring and guard requirements for different security zones?				
711	7.3	Do they include additional security practices such as physical construction or protection devices, for different security zones?				
For customer service area						
712	7.3.1	Is the reception area where the public applies for and receives travel documents built so that customers cannot have easy physical access to staff?				
713	7.3.1	Are there additional physical security measures in place such as screening, bullet-proof glass and duress alarm to protect employees?				
714	7.3.1	Are security personnel present during working hours?				
For restricted-access areas (Operation Zone and Security and High Security Zones)						
715	7.3.2	Are access control systems implemented such that access is subject to specific privileges applying to each staff member individually?				
716	7.3.2	Is employee access restricted to certain time periods i.e work shifts?				
717	7.3.3	Do access privileges to security and high-security zones require a two-factor authentication of the individual?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
718	7.3.3	Is the area where books are personalized placed under secure lock down at the end of every business day?				
719	7.3.3	Do access privileges to security and high-security zones require more than one so-privileged person in the zone at all times?				
7.4 Access Control and Monitoring						
720	7.4	Are all site facilities monitored by guards on a 24/7 basis?				
721	7.4	Are employees required to wear access privilege badges at all times?				
722	7.4	Do access privilege badges include clear photos of the bearer?				
723	7.4	Do access privilege badges have colours or other obvious codes to visually indicate the physical privileges of the bearer?				
724	7.4	Are visitors/contractors always escorted in all secure areas?				
725	7.4	Does this apply to employees who do not have the appropriate security clearance or whose position does not give access to certain zones?				
726	7.4	Is physical access controlled by physical and electronic means (locks, access privilege IDs, biometrics etc)?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
727	7.4	Are intrusion detection devices used (alarms, motion sensors, etc.) to trigger immediate attention of the guards?				
728	7.4	Are cameras and CCTV used in all external and internal door entry locations, and internal hallway and room areas?				
729	7.4	Are the video records from the monitoring equipment stored for appropriate periods (more than three months)?				
7.5 Other Physical Security Protection and Practices						
730	7.5	Is all mail, including travel document application and material received screened (X-Ray) in an appropriately located mailroom?				
731	7.5	Are facilities, assets and data protected against fire and other catastrophic losses?				
732	7.5	Are there arrangements in place for alternative sites and backup storage sites to ensure the continuity of operations?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 8 - Information Technology Security						
8.2 IT Security Policies and Practices						
801	8.2	Is there a comprehensive IT security policy in place?				
802	8.2	Is this policy up-to-date with regard to current technologies and practices?				
803	8.2	Is this policy implemented and practiced in full for travel document issuance IT systems, databases, and information flow?				
804	8.2	Does this policy refer to and incorporate current international standards such as ISO/IEC 27002:2005?				
805	8.2	Do these policies and practices include risk and vulnerability assessments, IT data privacy assessments, lost of data base information, unauthorized data access, and related assessments?				
806	8.2	Do the IT security policies and practices deal with appropriate **confidentiality** classifications of systems, databases and related information such that this information cannot be accessed, intercepted, or otherwise copied and obtained electronically by the wrong persons?				
807	8.2	Do the IT security policies and practices deal with appropriate **data integrity protection** of systems, databases and related information, such that this information cannot be changed, added to, or deleted except in the properly defined processes?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
808	8.2	Do the IT security policies and practices deal with appropriate **data availability** of databases and related information, such that this information cannot be blocked or hidden from legitimate users when it is required?				
809	8.2	Do the IT security policies and practices deal with appropriate **permissions of access** to systems, databases and related information, such that this information can only be accessed by **the authorized intended users** of the information?				
810	8.2	Have these policies, technologies and methodologies been evaluated by competent professional IT auditors to verify their efficiency and performance?				
811	8.2	Have technology products such as database software packages, servers, communications facilities, hardware security modules (HSMs), and other commercial products that are used, been certified at the appropriate Evaluation Assurance Level (EAL) security level?				
812	8.2	Have the cryptography devices used been certified to the appropriate level using international standards such as FIPS 140-2 or equivalent?				
8.3 User Security						
813	8.3.1	Do all users of the system and databases require at least a unique username and password sign-on in each case of such access?				
814	8.3.1	Are these individuals also limited by access and processing permissions to only certain application processes and to certain database records?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
815	8.3.1	Do all such sign-on sessions automatically terminate after short periods of inactivity?				
816	8.3.1	Can all accesses to the issuance IT system be monitored electronically?				
817	8.3.2	Does the TDIA deny Internet access to staff or contractors from any computer application PC or terminal used in the issuance process?				
818	8.3.2	Are such devices physically and technologically segregated (that is, either used for the application processing or for email and Internet)?				
819	8.3.2	Is there a program in place to randomly but regularly monitor email messages and Internet application accesses by all employees and contractors in order to detect matters or communications that may be of concern?				
820	8.3.2	Is the process very well protected by internal and strict privacy policies and practices, such that innocuous personal information learned from the monitoring is never released for any reason, and information that is not of security interest purged from records?				
8.4 IT Personnel						
821	8.4	Do IT personnel with physical access privileges to IT facilities, such as computer equipment rooms, physical databases, and communications facilities, have special access rights for entry to these facilities?				
822	8.4	Do these access privileges involve two-factor identification, such as a biometric measurement as well as a physical access token (such as an ID card)?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
823	8.4	Does access to these computer rooms or other physical IT facilities always require two or more authorized individuals at any time?				
824	8.4	Are IT Personnel responsibilities segregated and clearly defined so that no one individual ever has the right to overrule security policies and practices and make arbitrary decisions, make arbitrary backups of databases and other information files or in any way compromise the issuance system and its confidential information?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 9 - Protecting and Promoting Personnel and						
9.2 Security Clearances and Security Briefings						
901	9.2.1	Are all employees and contractors submitted to a background screening and reliability check corresponding to the classification level of the task (position) required?				
902	9.2.1	Are all staff positions assigned a classification or security level designation that recognizes the sensitivity of the position, responsibilities, access, and level of decision-making?				
903	9.2.1	Are these background and reliability checks carried out by or in collaboration with law enforcement, police or national security agencies?				
904	9.2.1	Do background and reliability checks for positions with higher security level classifications include a review of financial history and interviews with friends, family and colleagues?				
905	9.2.1	Are entitlement officers citizens of the issuing country?				
906	9.2.2	Are background and reliability checks repeated at appropriate intervals?				
907	9.2.3	Are secure areas delimited and internal controls in place to limit access authority of employees, both physically and electronically?				
908	9.2.4	Do temporary employees undergo the same background and reliability checks as permanent employees?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
909	9.2.5	Are all staff and contractors provided with an oral security brief and written guidelines on the TDIA's internal controls and security policies?				
910	9.2.5	Are all staff and contractors briefed on their access privileges and prohibitions attached to their security clearance level?				
911	9.2.5	Is there a written code of conduct and/values and/or an ethics code for all employees?				
9.3 Work Organization						
912	9.3.1	Are prescribed job functions established such that one employee cannot perform all the travel document entitlement and issuance functions?				
913	9.3.2	Do office flow procedures prevent the public from being able to select a specific employee?				
914	9.3.2	Are entitlement officers required to take the next batch of work in sequence?				
915	9.3.2	Do staff members rotate through several functions i.e. data entry, open mail etc.?				
916	9.3.3	Are all vital decisions and justifications made during the issuance process recorded in the file and database?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
9.4 Staff Morale						
917	9.4	Overall, has the TDIA implemented modern management principles to encourage a positive and healthy morale amongst all employees?				
918	9.4	Are the employment conditions and the pay structure and benefits for employees fair and competitive for similar work in other local sectors?				
919	9.4	Are there clear Human Resource (HR) policies in effect for employee reviews, pay raises, opportunities for promotions, and other HR matters?				
920	9.4	Are there formal HR mechanisms for employees to file personal treatment grievances and to have these grievances fairly heard and dealt with?				
921	9.4	Is there a high degree of job security at the TDIA for competent employees?				
922	9.4	Are all employees encouraged, with official recognition and other rewards, to make continuing recommendations for security and operational improvements?				
923	9.4	Are stratification conducted and analyzed regulary to gives the opportunity for employees to express, in a confidential manner, their satisfaction with their work and with the management practices of the organization?				
9.5 Investigations and Sanctions						
924	9.5.1	Are employees regularly reminded of the importance of being on guard and attentive to employee malfeasance and internal fraud including theft of documents, consumables and cash?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
925	9.5.1	Is there a documented policy requirement to have staff report all possible security violations without risk of negative feedback regardless of the nature of the violation or the individual involved?				
926	9.5.1	Are the sources of any such reports kept secret by the TDIA for the protection of reporting staff?				
927	9.5.2	Is there a formal official investigation process to investigate possible serious security breaches by employees at any level?				
928	9.5.3	Is this formal investigation process supported by clear and strong legislation such that offenders can be severely sanctioned if fault is found?				
929	9.5.3	Do these sanctions include immediate firing with loss of all benefits, if appropriate?				
930	9.5.3	Do these sanctions include criminal prosecution, if appropriate?				
931	9.5.3	Are results of investigations well publicized?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 10 - Lost and Stolen Travel Documents						
10.2 Prevention Measures						
1001	10.2.1	Are travel document holders made aware of the high security significance of the document and the need to keep it in a safe place?				
1002	10.2.1	Are travel document holders made aware of the importance of immediate reporting of a lost or stolen document?				
1003	10.2.1	Are there easy means of doing so such as well-posted toll-free numbers, fax, online, or in person?				
1004	10.2.1	Is the reporter of a lost or stolen document required to complete a written report?				
1005	10.2.2	Are there important incentives for the holder to take care of his or her travel document, such as: • higher fees for replacements; • requirement to appear in person for reapplication; • personal interview; • a mandatory endorsement identifying the travel document as a replacement; • mandatory hold times; • limited validity period of replacement travel document; • refusal to issue another travel document after a second lost travel document;				
1006	10.2.2	Are there careful entitlement checks done for the production of a replacement travel document?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1007	10.2.2	In the event of multiple loses, are lost and stolen claims subject to special investigations, including the possibility of a police investigation?				
10.3 Mitigation Measures						
1008	10.3.1	Are lost and stolen travel documents immediately cancelled and declared invalid for travel?				
1009	10.3.1	Do lost and stolen travel documents remain invalid if subsequently found by the rightful holder?				
1010	10.3.1	In this case, are they submitted to the TDIA for physical cancellation or destruction?				
1011	10.3.2	Are the travel document numbers stored in a national Lost and Stolen travel document database?				
1012	10.3.2	Are they so stored for at least as long as the validity period of the document?				
1013	10.3.2	Are lost or stolen blank passports reported in a national Lost and Stolen travel document database?				
1014	10.3.2	Is this database available to border control, immigration, visa, and law enforcement authorities?				
1015	10.3.3..1	Are lost and stolen travel documents reported to the Interpol SLTD?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1016	10.3.3..1	Are missing blank passports reported to the Interpol SLTD?				
1017	10.3.3..2	Are lost and stolen travel documents also shared with international partners and/or APEC RMAS?				
1018	10.3.3..2	Are missing blank passports reported to international partner and/or APEC?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 11 - Overseas Issuance						
11.2 Overseeing of Work						
1101	11.2	Are all overseas consular staff members and locally engaged staff who handle travel documents security screened to the same level as the personnel in the home country?				
1102	11.2	Does overseas staff receive the same training as the personnel in the home country?				
1103	11.2	Are policies, entitlement criteria, application requirements, etc. the same as in the home country?				
1104	1.3.2	Are all security policies and practices also fully and consistently implemented in all facilities and partner organizations that are involved with travel document issuance?				
1105	11.2	Are there constant communications between headquarters and missions to ensure policies and practices are known and applied?				
1106	11.2	Are audits and spot checks performed on a regular basis to ensure that all policies and practices are being enforced overseas?				
11.3 Entitlement						
1107	11.3	Does a supervisor who is a citizen of the issuing country always approve the final entitlement decision?				
1108	11.3	Do the missions have access to the same clearance, watch lists and travel restriction databases as domestic offices?				
1109	11.3	Are any difficult cases referred to headquarters?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1110	11.3	Are travel documents issued at missions included in national databases?				
11.4 Personalization						
1111	11.4	Are the books personalized overseas with the same personalization (printing) technology and stock, including security features as the books produced in the home country?				
1112	11.4	Do only the officers responsible for travel document issuance have access to blank books?				
1113	11.4	If locally engaged staff is able to personalize travel documents, are these always checked by senior consulate staff who are citizens of the country before release?				
1114	11.4	For travel documents personalized overseas in consulates, are all steps proposed in Chapters 4 and 5 for handling, accounting and storage of blanks also fully implemented in the missions abroad?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
Chapter 12 - National and International Stakeholders						
12.2 National Stakeholders						
1201	12.2	Does the TDIA have active partnerships with other national authorities that are stakeholders in the issuance and use of travel documents?				
1202	12.2.1	Does the TDIA exchange information with border control and immigration authorities on the development, design and integration of security features in travel documents?				
1203	12.2.1	Does the TDIA exchange information with border control and immigration authorities on document fraud and security threats?				
1204	12.2.1	Does the TDIA exchange information with border control and immigration authorities to ensure interoperability with existing and future border systems and infrastructure;				
1205	12.2.1	Does the TDIA, border control and immigration authorities share data to include in watch lists and travel restrictions lists?				
1206	12.2.2	Does the TDIA exchange information with law enforcement, police and forensic document laboratories regarding travel document fraud and security features?				
1207	12.2.3	Does the TDIA exchange information regarding document versions and security features with Vital Statistics organizations issuing breeder/primary and supporting documents used in the entitlement?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1208	12.2.4	Does the TDIA exchange information with other national organizations involved in the travel document issuance process, e.g. overseas issuance, diplomatic/special/official passport issuance, accepting applications?				
12.3 International Partners						
1209	12.3	Does the TDIA have active partnerships and associations with other nations and international organizations?				
1210	12.3.1	Is the TDIA aware of the role of the ICAO MRTD program?				
1211	12.3.1	Does the TDIA participate in ICAO TAG/MRTD and its working groups (NTWG and ICBWG)?				
1212	12.3.2	Does the TDIA participate in international data exchange networks such as Interpol LSTD, APEC RMAS or others?				
1213	12.3.2	Does the TDIA participate in regional and international partnerships to share data and information and review threats, frauds, counterfeiters, security features and security practices?				
1214	12.3.3	If required, is the TDIA aware of travel document capacity building programs, help, funds and expertise available?				
12.4 Private Partners						
1215	12.4.1	Does the TDIA share information with airlines and associations that verify travel documents to determine the right to board a plane and communicate advance passenger information?				

No.	Section	Question	% Compliance	Remarks on Gaps and Mitigation Measures	Risk H/M/L	Risk Score
1216	12.4.2	Does the TDIA share information with ISO and/or private companies to remain aware of latest developments in travel document technologies, systems and processes?				
1217	12.4.2	Does the TDIA undertake regular Requests for Information to remain aware of latest research and innovations?				