Appendix A

Detailed findings and action plan

Action plan and progress

Recommendation	Agreed action	DBS Owner	Progress	Date complete
a02 and a03. DBS should ensure that the policies and procedures currently in place, that are being provided to staff and that they are expected to follow, are reviewed and updated in line with the documented requirements.	**Partially Accept**	**Director PWF**	The original implementation date for this recommendation was 30/12/16 however to ensure appropriate communication of the seven staff facing policies they were grouped to enable the publication to be supported by focused corporate messages on the specific policy areas and staff drop in sessions. 2 were published in December 2016, a further 2 in January 2017 and the remaining 3 were published in February.	28/02/17
a04. As DBS' new policies were created over a year ago, DBS should ensure that they are further reviewed, ahead of roll out of R1 in December 2016, to ensure they are adequate and effective and still fit for purpose before obtaining approval and disseminating to staff. In addition, the roll out of the new Information Security policies and procedures should be accompanied by an awareness raising campaign to help ensure that staff are aware of these new procedures and how compliance with them will be monitored.	**Partially accept**	**Director PWF**	Publication of the remaining information security policy set has been included for review in the project plan for publication two months prior to R1 (Barring) Go-Live. As set out for a02 & a03 implementation of the policies is supported by comprehensive publication and awareness arrangements. These will be tailored to the types of audience using the policies as some are more technical in nature and as such are not applicable to all staff. Staff understanding of their responsibilities will be tested via e-learning packages with the successful completion being provided to the SIRO. Completion of the e-learning is supported with mandatory staff face-to-face training sessions. Anyone not obtaining an 80% pass mark for the e-learning will be invited to attend a further briefing session.	
a06. Once R1 is in place, review the written policies and procedures to ensure that the status and applicability of all such documents are clear to staff.	**Declined as a recommendation treated as an observation.**	**Director PWF**	The staff facing policies will be reviewed on an annual basis as part of business as usual operational security. This has been included in the development of the internal Assurance Framework. Oversight of staff understanding is assessed via the proof of learning results from e learning completion. Directors will be asked to confirm assurance as part of annual governance reporting	N/A
a08. Develop a policy log that maintains details of the various policy and procedure documents, including document owners and	**Partially accept**	**Director PWF**	Action complete A Log of all ISMS policies and Information governance Policies is in place and has been updated to include the additional aspects contained in this recommendation	31/12/16

Recommendation	Agreed action	DBS Owner	Progress	Date complete
review schedules.				
a16. Once R1 is in place DBS should ensure that there is a central repository of all policy and procedure documents that is easily accessible to all staff and that is kept up to date.	**Declined as a recommendation treated as an observation.**	**Director PWF**	Policies are currently published on internal intranets with a library held which is available to all staff. Once R1 is in place the library will be accessible via a single intranet. The policies will be reviewed and updated in accordance with their review schedules.	22/12/16
a22, a23, a24 and b08. A DBS specific PIA policy and framework should be created to ensure that PIAs are undertaken for all projects, or process changes, that involve the processing of personal data by DBS. The policy should set out a clear process for determining when a PIA should be conducted, who it will be authorised by, how it will be incorporated into the project plan and how compliance will be monitored. The policy should clearly identify the roles responsible for completing PIAs.	**Declined as a recommendation treated as an observation.**	**Director PWF**	Undertaking PIAs is now formally documented in the Data Sharing Policy which incorporates the Home Office PIA guidance previously used.	03/02/17
a31. As part of the training review DBS should review the CSL course content to ensure that it continues to meet their needs and, if it doesn't, they should seek to source more suitable training.	**Declined as a recommendation treated as an observation.**	**Director PWF**	The CSL course is a cross government e-learning package that is owned by the Cabinet Office and DBS is mandated by the Home Office to undertake this annually. DBS do not have the authority to amend the CSL course however we have worked with the Home Office to produce a DBS specific e-learning package which will be hosted on the Home Office learning and development platform.	N/A
a33 and a34. DBS should devise and deliver a centralised training plan on an annual basis, which includes completion of a specific training needs analysis to identify all staff and third parties who process personal data and have specific role based training needs. **See recommendation a39, a41 and b07**.	**Partially Accept**	**Director PWF**	Analysis undertaken for the annual face to face training has been used to develop the individual modules to enable managers to select those applicable to the work their staff undertake these will be in addition to those that are mandated for all staff to complete.	
a38 and a39 See Recommendation **a33 and a34:**	**Partially accept**	**Director PW**	Course identified and training is being scheduled.	
a43. Introduce regular audits of the movers and leavers process and ensure that accounts/access permissions have been amended or deleted promptly. This will	**Partially accept**	**Director PWF**	Audit activity included in the Assurance Framework to ensure accounts and access permissions are in line with staff moves and departures.	

Recommendation	Agreed action	DBS Owner	Progress	Date complete
ensure that staff are only able to access information on a 'need to know' basis and that permissions are removed in a timely fashion. Periodic reconciliations should also be undertaken with current HR records to provide assurances that staff are only granted correct access levels and unnecessary access is removed. Ensure that the HR Staff Departure Procedure is reviewed and updated to include this recommendation.				
a53 and a54. See Recommendation **a43.**	**Partially accept**	**Director PWF**	Leavers Policy currently undergoing review. The Information Governance Security Manager (IGSM) authorises all access and removal from uCRM. This has now been formalised by the inclusion of the audit activity within the assurance framework.	
a59 and a60 See recommendation **a04.**	**Partially accept**	**Director PWF**	See progress comments as per progress a04 update	
a64 See recommendation **a118.**	**Partially Accept**	**Director PWF**	Risk review scheduled.	
a94. Once R1 is in place, ensure that the DBS Security Assurance Framework operates effectively and that monitoring is undertaken against the Baseline Control Set and is reported appropriately.	**Declined as a recommendation treated as an observation.**	**Director PW**	The suitability of the Security Assurance Framework post R1 will be reviewed as part of the ongoing business as usual operational security. The existing Assurance Framework has been uplifted to conform with ISO27001/13 which will be used at the time R1 is implemented to ensure the Baseline Control Measures operate effectively with quarterly reports on this to be provided to the responsible directors.	N/A
a101. DBS should revisit the IT Health Check, once R1 is rolled out, to ensure that the risks have been addressed. Any remaining risks should be re-evaluated and, where appropriate, mitigated. See finding **a122**.:	**Partially Accept**	**Director PWF**	Accreditation plays a key role in all IT project implementations with the risks identified as a result of IT Health Checks being reviewed by the Senior Information Risk Owner as part of the project approval. Any risks tolerated at the point of go-live are kept under regular review as part of operational security management. IT Health Checks are conducted as part of any system changes or on a two yearly basis whichever is sooner to ensure any risks are identified and address as in line with the organisations risk appetite.	26/01/17
a106. Once R1 is in place, undertake a review to ensure that Backup and Restoration Procedures are in place for all key information systems.	**Declined as a recommendation treated as an observation.**	**Director PWF**	Development is ongoing for the Disaster Recovery (DR) of R1. DR is a mandatory acceptance criteria which must be satisfied prior to the implementation of R1.	N/A
a108. Backups should be regularly tested to ensure that systems can be safely restored.	**Declined as a recommendation treated as an observation.**	**Director PWF**	See progress comments as per a106	N/A
a117. DBS should also have a	**Accept**	**Director**	DBS Security was involved in the set up of Security Operating Centre (SOC),	

Recommendation	Agreed action	DBS Owner	Progress	Date complete
role in ensuring that monitoring is being carried out appropriately and that the reports that they receive from TCS are fit-for-purpose and allow them to maintain sufficient oversight.		**PWF**	including contractual requirements. Weekly reports are being provided to the DBS Accreditor and the Operational Security manager.	
a118. DBS should keep the legacy system under review as R1 progresses towards roll-out and consider whether further action in this area is required if roll-out is delayed or if they remain comfortable to accept the risk. See finding **a64, a92 and a130**.	**Partially Accept**	**Director PWF**	The risk has been considered and is be tolerated by the SIRO as low risk. Further review of this risk would form part of a wider risk assessment that would be undertaken should the situation arise.	N/A
a130. See recommendation **a118**	**Partially accept**	**Director PWF**	**Please see comments against progress for a118.**	N/A
b03a. The DBS should consider creating a data sharing steering group to discuss any new data sharing proposals or changes to existing data sharing agreements for disclosure and barring data. The steering group should include representatives from the Information Governance team, to provide an insight into the data protection implications. **b03b.** Formally document all data sharing decisions or comments discussed for audit, monitoring and investigation purposes.	**Partially Accept**	**Director PWF**	**Recommendation complete.** A Data Sharing Forum has been established which has responsibility for reviewing data sharing agreements.	12/01/17
b04. Recommendations or comments provided by the IGSM in relation to the data sharing project should be formally recorded. See recommendation **b03b.**	**Partially Accept**	**Director PWF**	**Recommendation complete.** A formal review process now forms part of the Data Sharing Framework with the IGSM as part of the review panel.	12/12/16
b05. Ensure that the final sign off provided by the SIRO is formally documented. See recommendation **b03b.**	**Partially Accept**	**Director PWF**	**Recommendation complete.** Formal approval of all MoUs by the SIRO is specified in the Data Sharing Policy.	12/12/16
b06. Implement a clear data sharing process for both disclosure and barring information. The agreed data sharing process should be clearly documented in a policy. The policy should clearly state who has the authority to make systematic and one- off data	**Accept**	**Director PWF**	**Recommendation complete.** The process is documented in the Data Sharing Policy.	12/12/16

Recommendation	Agreed action	DBS Owner	Progress	Date complete
sharing decisions and when it is appropriate to do so. Ensure that the policy is communicated to all staff and reviewed regularly to reflect any changes.				
b07. Provide specialised data sharing training to all staff involved in making informed decisions regarding data sharing or disclosures of data. Carry out a training assessment to identify role-based training needs for staff. See recommendation **a33** and **a34**.	**Partially Accept**	**Director PWF**	Analysis undertaken for the face to face training has been used to develop the individual modules to enable managers to select those applicable to the work their staff undertake these will be in addition to those that are mandated for all staff to complete.	
b08. See recommendation **a24**, the requirement to conduct a PIA involving data sharing, should be documented in a DBS policy.	**Partially Accept**	**Director PWF**	**Action complete**	12/12/16
b09. Revisit outdated PIAs to reassess privacy risks and solutions. PIAs should be completed for all new data sharing projects or existing data sharing projects where a significant change is involved.	**Partially Accept**	**Director PWF**	**Recommendation complete** The requirement to conduct PIAs is contained in the Data Sharing Policy.	12/12/16
b11. The Information Governance (IG) team should be involved in conducting PIAs with the business areas. All PIAs carried out should be held centrally by the IG team once completed.	**Partially Accept**	**Director PWF**	**Recommendation complete** The IG team is included in the formal review process for PIAs under the Data Sharing Policy	12/12/16
b14. The nominated department (see recommendation **b11**) should maintain a log of all PIAs carried out by the DBS. The log should record the reason that the PIA was carried out and the outcome. Approval or rejection dates should also be logged.	**Accept**	**Director PWF**	**Recommendation complete** Under the Data Sharing Policy the IG team is responsibility for maintaining the central log.	12/12/16
b15. Ensure that the data sharing policy (see recommendation **b06**) sets out that a data sharing agreement is required to be in place when systematically sharing information. The policy should also require an oversight process to ensure that an information sharing MOUs log is maintained and that there is a regular review process.	**Accept**	**Director PWF**	**Recommendation complete** **The aspects detailed in the recommendation are documented in the Data Sharing Policy.**	12/12/16
b19. Create a standardised MOU for information sharing to ensure	**Partially Accept**	**Director PWF**	**Recommendation complete**	12/12/16

Recommendation	Agreed action	DBS Owner	Progress	Date complete
that MOUs are consistent across the DBS.			**Standard MoU template documented in the Data Sharing Policy.**	
b24a. See recommendation **b15**. The log should be maintained by the nominated department responsible for holding information sharing MOUs. **b24b.** Information sharing MOUs that have not yet been signed by third parties should be followed up and signed by a senior member of the organisation.	**Partially Accept**	**Director PWF**	**Recommendation complete** Under the Data Sharing Policy the IG team is responsibility for maintaining the central log.	12/12/17
b25a. Review MOUs and include the right for the DBS to conduct audits of third party organisations receiving DBS data. Audits should be carried out to seek assurance that the requirements on the MOU are adhered to. **b25b.** Once carried out, these audits should be formally documented.	**Partially Accept**	**Director PWF**	**Recommendation complete** Audit requirements are included in the data sharing process and MoU template.	12/12/16
b31. Review information sharing MOUs to include arrangements as to how the data will be shared with the third party.	**Partially Accept**	**Director PWF**	**Recommendation complete** Recommendation details are captured under the Data Sharing Policy.	12/12/16
b34. Include the requirement to report security incidents or near misses in the MOUs. This should clearly set out the process to follow when reporting a breach and who to contact.	**Decline**	**Director PWF**	The requirement to report security incidents or near misses is already documented in existing MoUs. This has been incorporated in the MoU template.	N/A
b42. Where a request for disclosure is received and information regarding the individual is held on the uCRM, a note should be added to the case file which records that a request has been received, who has dealt with the request, what information has been released and the legal basis for disclosure.	**Partially accept**	**Director JM**	**Recommendation complete.** A note will be added to the case files to record the details specified in the recommendation.	28/02/17