Disclosure and Barring Service

Data protection audit report

Information Commissioner's Office

Auditors:	WITHHELD **–** Team Manager WITHHELD - Engagement Lead Auditor WITHHELD – Lead Auditor
Data controller contacts:	WITHHELD **-** Head of Security and Facilities/Deputy SIRO WITHHELD **–** Information Governance and Security Manager
Distribution:	**Paul Whiting** – Chief Financial Officer/SIRO WITHHELD **-** Head of Security and Facilities/Deputy SIRO WITHHELD **–** Information Governance and Security Manager
Date of first draft:	5 September 2016
Date of second draft:	10 October 2016
Date of final draft:	09 December 2016
Date issued:	**December 2016**

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of the Disclosure and Barring Service.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

Contents

1. Background page 04
2. Scope of the audit page 05
3. Audit opinion page 06
4. Summary of audit findings page 07
5. Audit approach page 09
6. Audit grading page 10
7. Detailed findings and action plan page 11
8. Appendix A page 68

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 In February 2014 the Disclosure and Barring Service (DBS) self-reported an information security breach which occurred in Barring Operations, Darlington. (ICO case reference ENF0531715). The breach involved a closed case summary containing sensitive personal data being mistakenly sent to another individual. The ICO Enforcement Department conducted an investigation and this resulted in a recommendation that a consensual audit would be the most effective way of improving compliance within DBS.

1.4 DBS is a non-departmental public body (NDPB), sponsored by the Home Office (HO) and replaced the Criminal Records Bureau (CRB) and Independent Safeguarding Authority (ISA). They employ 270 staff in Darlington and process 100,000 records which are predominantly held in paper form.

1.5 TATA Consultancy Services (TCS) maintain the legacy systems CRM and uCRM from the organisations that were merged to form DBS, the Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA). A new single case management system R1 is being developed for all DBS Operations on one modernised platform. R1 will be an internet facing portal for Basics, Regulatory bodies, Disclosure, Barring, Applicant, Referring organisations and the public. R1 was originally due to be implemented across DBS in the summer of 2015 however it was subject to a number of delays. Whilst we were on site we were informed the release date was scheduled for December 2016. However, subsequent to the audit we were advised that the release date has been further delayed and there is currently no definite date for release.

1.6 It was recognised that the ongoing work in relation to the development of R1 meant that the audit was likely to identify areas of weakness that had already been identified by DBS. In some areas activities had already commenced and for those relating to the development of the new IT system, requirements had been captured in the contract and were already included in the system technical designs.

1.7 An introductory meeting was held on 7 June with representatives of the DBS to identify and discuss the scope of the audit.

2. Scope of the audit

2.1 Following pre-audit discussions with DBS, it was agreed that the audit would focus on the following areas:

a. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

b. Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and DBS with an independent assurance of the extent to which DBS, within the scope of this agreed audit is complying with the DPA.

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

3.3 Overall Conclusion	
Limited assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non- compliance with the DPA. We have made two limited assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report.

4. Summary of audit findings

4.1 Areas of good practice

A Risk Management Framework is in place along with comprehensive departmental and corporate risk registers which are regularly updated with actions and reported to Senior Management Team and Risk Improvement Forum monthly and the Audit and Risk Committee quarterly.

All staff at DBS are mandated to undertake the annual Civil Service Learning on Handling Information on induction and as refresher training. In 2015 the Data Protection Officer and Information Governance and Security Manager developed and delivered bespoke training sessions covering data protection and information security, which DBS plan to roll out again by the end of 2016 and annually thereafter; attendance is mandated by the SIRO.

A comprehensive clear desk procedure is in place, at the end of each day desks are cleared of all paper records containing personal data and secured in lockable filing cabinets or safes overnight. Regular sweeps are undertaken to ensure compliance.

There is a robust process in place for ensuring the correct printed material is sent securely to the correct person and address. This includes double checking all pages, validating the address, double enveloping and sending via recorded or special delivery.

4.2 Areas for improvement

A Privacy Impact Assessment (PIA) policy and framework specific to DBS processing of personal data is yet to be established to ensure PIAs are undertaken before entering into a third party supplier relationship, the introduction of a project, or significant change to a procedure involving personal data.

There was a lack of awareness amongst staff of where the current information breach incident procedure is stored and its contents this includes what is expected of them in respect of the reporting of all types of information security incidents.

Training needs have not been assessed for all staff groups to ensure that the level of training provided is appropriate to the data handling responsibilities of those groups. Refresher training is completed annually via Cabinet Office eLearning. Therefore there is a risk that staff knowledge of information management is not maintained or updated and there is an insufficient level of assurance that staff have understood the training content.

Where third party contractors are utilised to collect, process or dispose of personal data on behalf of DBS, there should be a comprehensive contract in place which clearly sets out requirements and obligations in relation to information security and provides a right of inspection to DBS representatives.

Current information security policies are aligned to comply with ISO 27001:2005 standard. However, some policies aligned to ISO 27001:2013 are still in draft form and have yet to be disseminated to staff. A number of policy review dates have passed and are now overdue. There is currently no Policy log in place to allow oversight of policy documentation to be maintained.

There is no policy or procedure in place to clearly set out the data sharing process or the processes to be followed for both disclosure and barring information. Responses to information disclosure requests are not authorised by a senior member of staff before they are released. There was a lack of awareness amongst some staff interviewed regarding the legislation that permitted the DBS to release data to a third party.

5. Audit approach

5.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

5.2 The audit field work was undertaken at DBS (Barring Operations) Stephenson House, Morton Palms Business Park, Alderman Best Way, Darlington DL1 4WB between 16 and 18 August 2016.

6. Audit grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Recommendation priority	Definitions
	High assurance	Minor points only are likely to be raised	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non compliance with the DPA.
	Reasonable assurance	Low priority	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA.
	Limited assurance	Medium priority	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA.
	Very limited assurance	High priority	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

Detailed findings and action plan

7.1 Scope: Security. The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

Risk: Without robust controls to ensure that personal data records, both manual and electronic, are held securely in compliance with the DPA, there is a risk that they may be lost or used inappropriately, resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

Policy

a01. In 2013/2014 DBS introduced a One Way of Working (OWoW) project to align the policies of the previous CRB and ISA organisations. The objective was to create a single set of DBS policies to ensure that DBS functions were supported, efficient and effective.

a02. Current information security policies are aligned to comply with ISO 27001:2005 standard. However, some policies still record the previous Senior Information Risk Officer (SIRO) and the review dates have passed and are now overdue.

a03. For example the following policies are provided to new starters as part of their induction and welcome pack:

- Clear Desk Policy DBS 123 v1 (due for review March 2015)
- Internet and Email Policy DBS 130 (due for review Dec 2014)

We were informed that these policies will be superseded with new policies once R1 has been rolled out.

Recommendation:

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.

Management response: **Partially Accept**

Action: DBS had already identified that the ISMS required uplifting from the ISO 27001:2005 standard to ISO 27001:2013 standard. The work commenced in May 2015 and all policies and procedures have been reviewed to uplift them to comply with 27001/2013 standard. A conscious decision was taken by DBS not to publish these Policies until R1. Due to a delay in the implementation of R1 DBS reviewed this decision and staff facing policies will be communicated to staff by 31/12/2016. Technical policies that current systems are unable to comply with will be published at R1 implementation The 2005 policies referred to are still in place, valid and being followed by staff until the new policies are published and communicated.

Implementation date & owner: **31/12/16 WITHHELD**

a04. There is a comprehensive suite of information security policies, which have been created, reviewed and approved jointly by TCS and DBS. They are aligned with the ISO 27001:2013 Standard with a view to achieving certification. However, they have yet to be disseminated to staff. We were informed the delay in their publication is due to the implementation of R1 being further delayed from the original timeframe of summer 2015.

Recommendation:
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.

Management response: **Partially accept**

Action: DBS had already identified the requirement for an uplift as per a02 & a03 response above and the work commenced on this in May 2015. A conscious decision was taken by DBS not to publish these Policies until R1. Due to a delay in the implementation of R1 DBS reviewed this decision and staff facing policies will be communicated to staff by 31/12/16. Technical policies that current systems are unable to comply with will remain to be published at R1 implementation.

Implementation date & owner: **31/12/16, WITHHELD**

a05. There is a TCS Operations Policies and Procedures document which covers management and operation of the information processing facilities that TCS have implemented for the delivery of the DBS service.

a06. It was reported that there are approximately 30 documented policies in place. These consisted of DBS documents, TCS documents and jointly-owned documents. There was some evident confusion regarding the status and applicability of some of these documents.

Recommendation:
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.

Management response: **Decline**

R1 was not within the scope of the ICO audit and therefore this recommendation is rejected. However DBS will take this recommendation as an observation for the implementation of R1. As a matter of BAU all policies both for DBS and TCS are reviewed as required to ensure they are fit for purpose.

a07. Some policy documents have been drafted in anticipation of the roll-out of the new R1 system and do not apply to the uCRM system.

a08. There is currently no Policy log in place to allow oversight of policy documentation to be maintained.

Recommendation:
a08. Develop a policy log that maintains details of the various policy and procedure documents, including document owners and review schedules.

Management response: **Partially accept**

Action: We have an existing log that we will expand to reflect the owners and review schedule.

Implementation date & owner: **30/12/16, WITHHELD**

a09. There are a number of information security and risk working/steering groups and board meetings such as:

- Information Security Forum (ISF) that meets quarterly and is chaired by the SIRO and TCS;
- Security Working Group (SWG) meets monthly;
- TCS OpSec Assurance quarterly meeting.

a10. We were not provided with any minutes or records to demonstrate a formal process for the approving, publication or review of new policies. We were provided with minutes for an ISF meeting at which the IS Policy was approved; however, this did not appear to be part of a formalised process.

Recommendation:
a10. DBS should ensure that there is a formal consistent documented process for policy approval, publication and dissemination.

Management response: **Decline**

Action: The information security and risk working/steering groups and board meetings monitor the development and review of policies and procedures to provide assurance that they have been approved and will provide sign-off

where appropriate. However, approval by these meetings will only involve a very small number of policies as the majority are reviewed and approved in line with agreed change management process with sign-off by the designated authority level, this includes the SIRO and Deputy SIRO dependant on the nature of the policy.

A formal approach is taken for all data protection/information security related meetings; ToR are in place that include standing agenda items for each meeting which are supplemented by additional items as necessary depending on the specific business needing consideration. Minutes and action logs are also produced.

a11. New policy documents are made available to staff by email. Staff reported that they can retain copies of the documents in their personal section of the DBS network. However, they are encouraged not to do this.

a12. New policy documents are also highlighted in monthly team briefings which are circulated to all managers. Managers reported that can choose to forward these briefings to their staff, or they can choose to hold team meetings where they can discuss the contents in more detail, if they think it necessary or appropriate. Managers are required to hold team meetings on a monthly basis, as a minimum.

a13. In addition, Operational Bulletins are issued to managers two or three times a week. These bulletins can be used to circulate information about policies and procedures.

a14. Where a document is subject to minor amendments, these changes will be highlighted in bulletins or briefings rather than the whole document being circulated again.

a15. While staff maintain their own copies of policy documents, in many cases, the main repository is on the intranet as hosted on the POISE network. However, it was reported that the majority of staff do not need to access POISE on a regular basis for their day-to-day work; they would access it for HR purposes.

a16. It was reported that the key security policies and staff guidance documents are also stored on the iGap intranet, which is hosted on the secure network, which operational staff use more frequently.

Recommendation:
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.

Management response: **Decline**

Action: R1 was not in the scope of the ICO audit however DBS already stores all policies in a central repository accessible to all staff. However DBS will take this recommendation as an observation for the implementation of R1 and our current approach will be further refined once R1 is in place as part of BAU as all staff will use and access one IT platform which will contain the central repository.

Organisation

a17. We were provided with a small number of job descriptions for staff involved in handling sensitive personal data. The content was inconsistent and the documents still carried the ISA logo, they did not appear to have been reviewed or updated, with current roles and responsibilities since 2010.

Recommendation:
a17. DBS should review all job descriptions and ensure that the organisation structure, reporting lines, ownership and responsibilities are clearly documented, up to date, approved by line management and accessible to all staff.

Management response: **Decline**

Action: DBS do not use job descriptions in this way. Job Descriptions are reviewed as and when a role is advertised. All staff have a Personal Development Review document which details their main objectives and responsibilities. These are reviewed with the line manager at the start of each reporting year and as a minimum at the midpoint in the year and feedback provided. When DBS was established in 2012 all staff received a letter confirming their job role had transferred to DBS.

a18. There is a Risk Management Framework in place that includes Governance, Assurance, Risk management process and Risk Management reporting.

a19. Business/Department risks feed into the DBS Corporate risk registers; they contain a variety of information security risks. All risks record the owner, title, description, cause, effects, core controls and BRAG rating. They are reviewed monthly and updated this includes: assessment, progress, actions, action owner, implementation date and if complete. Reports are provided on a quarterly basis to the ARC.

a20. Information Asset Owners (IAO) are in place and each is responsible for a number of information assets. Assets include spreadsheets of mostly casework personal data, information that supports the business needs, actions, exchanges and post received logs.

a21. New assets should not be created without authorisation from an IAO. New assets, amendments or deletions automatically populate an email to the Information Governance and Security Manager (IGSM) or Data Protection Officer (DPO) to authorise the action. All assets are recorded on an Information Asset Database (IAD) by the IAD Coordinator and risk assessed quarterly. A declaration is sent by the IAO to the IGSM and DPO to confirm that their allocated assets have been reviewed.

a22. DBS use the HO Privacy Impact Assessment (PIA) Policy, which was effective from May 2010. This is a high level policy specific to the HO's collection, creation, storage and use of information as a Data Controller. The policy includes links to other guidance and HO policies including the ICO PIA guidance.

a23. In terms of the DPA, DBS are a Data Controller in their own right; they decide the manner and purpose for processing the sensitive personal data, which differs from the HO; they do not currently have their own PIA Framework. However, there was evidence that PIAs were conducted as a result of the Protection of Freedoms Bill 2012, when DBS became the successor body.

a24. PIAs are not consistently undertaken before the introduction of a project, or significant change to a procedure, involving personal data. We were informed that this was due to the changes not being broad enough on legacy systems. DBS have used the HO policy and the PIA guidance on the ICO website to undertake a PIA of the new R1 system.

Recommendation:
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.

Management response: **Decline**

Action: DBS currently use Home Office PIA Policy and framework the content of which is in line with ICO guidance. DBS has reviewed the policy and associated documentation and are content that it is fit for purpose without the need for a specific DBS policy. Where there are major changes a PIA is undertaken as part of the project, for example R1. We currently have a programme of work underway (which had already commenced at the time of the audit) that will put central governance arrangements in place within the Information Management team this will include the requirement to consider the need for a PIA.

a25. The Data Management Group (DMG) was formed two years ago their remit is to focus on assurance and improve the data integrity, and handling of data throughout the whole of DBS. All initial objectives and actions have been delivered. The format of the DMG has been reviewed to have a more strategic focus and new terms of reference have been approved by SMT. The first meeting is scheduled for 15 September.

a26. A Data Road Map (DRM) presentation, covering an 18 month period starting July 2016, was agreed on 30 June at the Strategic Board and by the SMT in July. The DRM will enable DBS to produce management information, and trend and data analysis to improve the services and safeguarding in a less resource intensive

manner. The work will operate under the DMT for oversight but managed by a working group led by the Head of Security.

a27. It was reported that there are a number of working/steering groups and meetings that have data protection and information governance within their remits (see **a09**); however the remits of these groups did not appear to be formally documented and it was difficult to ascertain where certain responsibilities lay. For example, we were provided with SWG minutes for May and June 2016 but it did not appear that information security risks, incidents, breaches or near misses were on the agenda and they did not appear to be discussed.

Recommendation:
a27. DBS should ensure that data protection meetings have documented TORs and agendas; meetings should be minuted.

Management response: Decline

Action: Refer to management response a10. SWG (Chaired by the HoSaF) oversees R1 development and until recently the project did not have access to personal data. However, in very limited circumstance, for example data migration, the project now requires access to citizen data. Where this is needed a Security Case is developed which considers the risks to the data and is approved by either the SIRO or the Deputy SIRO.

The SWG minutes provided at the time of the audit stated that a separate meeting was being held to discuss the project security and information risks as a full review was being undertaken and there was an action to cover this point.

The review of security incidents and breaches is covered under the standing agenda item at the monthly Operational Security meeting chaired by HoSaF.

Training and Awareness

a28. DBS employs permanent and temporary staff on fixed term contracts, all staff groups are subject to the same training. However, only permanent staff are employed in the operational area of the business where the majority of the processing of sensitive personal data takes place; they are required to be vetted to SC level. We were provided with evidence post audit that staff are required to sign legal agreements on appointment that include confidentiality and information security.

a29. Learning and Development (L&D) provide the DBS corporate induction which includes the issue of a welcome pack to each individual containing a number of information security polices and a Code of Conduct. Staff are required to sign an attendance sheet to confirm that they have attended the induction session. Line Managers also provide their staff with some induction training but the standard is inconsistent across DBS.

Recommendation:
a29. To provide management with evidence that all staff are made aware of their responsibilities, with regard to processing records containing personal data, introduce a requirement for staff to confirm that they have read and understood the relevant policies.

Management response: **Decline**

Action: All relevant policies are communicated to staff via team brief by line managers who cascade the information and direct staff to the appropriate areas if further clarification is required. Team brief is mandatory that it is delivered within a set time frame and feedback is also passed back to Comms. All staff are aware they have a responsibility to ensure that they understand how to handle data within their specific job role. This knowledge is refreshed annually via mandatory face to face briefing sessions, completion of e-learning, both of which are recorded, and locally held drop in surgeries that includes legal advice.

a30. Staff must undertake the Civil Service Learning (CSL) eLearning "Responsible for Information" as part of their induction training and then annually as refresher training. The course covers information security; the candidate must work through the sections and complete the final assessment with a minimum pass mark of 80%,

if this mark is not attained then the assessment must be retaken. The pass certificate is printed and provided to the Line Manager after which it is placed on the individual's HR file.

a31. It is believed that the content of the CSL course has not changed since it was first introduced. It is possible for the candidate to go straight to the assessment without working through any of the sections. This does not ensure that the training is effective and understood by staff. We were advised that the CSL course was under review.

Recommendation:
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.

Management response: **Decline**

Action: This training is developed and mandated by the Cabinet Office for all government departments/bodies and is refreshed and deemed appropriate by Cabinet Office on behalf of Government. DBS has already previously identified areas requiring further training and supplement this training with DBS specific training depending on the role, e.g. caseworkers, and mandatory annual briefing sessions to ensure staff understand their responsibilities. At the time of the audit we were already in discussion with the Home Office to secure amendments to the e-learning package they had developed to ensure the content was amended to make it relevant to DBS prior to mandating its completion by all staff which is in addition to the mandated Cabinet Office elearning.

a32. Each business area has a number of specialised processes and procedures in place. Also a number of staff at various levels have specific specialisms and are responsible for documenting individual processes in "Desk Instructions". These instructions are very detailed and provide a comprehensive step-by-step guide of the process to be carried out. The content references relevant legislation as well as organisational policies and procedures. They are regularly updated; version controlled and stored on the iGap database along with other user facing policies and procedures.

a33. We were informed that there is currently no long term training strategy or any training needs analysis being conducted. However, we were advised that DBS are in the early stages of reviewing all current training, for both Liverpool and Darlington, including the CSL course; this will involve HR reviewing the end-to-end recruitment process.

a34. There is no specific role-based training provided to staff who process the most sensitive personal data. All staff interviewed confirmed that the training for their specific role consists of shadowing, mentoring, and peer-to-peer "on the job" training by a more experience member of staff within their team.

Recommendation:
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**.

Management response: **Partially Accept**

Action: At the time of the audit DBS had already identified the requirement for a centralised training plan, work had already commenced in conjunction with L & D team to include a Training needs analysis specific to staff roles and responsibilities. Within the Barring function there are a number of roles already covered by a training needs analysis. DBS has previously reviewed the suppliers training to ensure it is in line with that undertaken by our staff. Within our barring function we currently undertake several job role specific training which incorporates data handling, redaction and data sharing as appropriate to the role. We will extend this approach to take account of the data handling roles across the organisation.

Implementation date & owner: **31/12/16 L&D**

a35. To supplement the CSL course the DPO and IGSM have designed and delivered mandatory face-to-face Data Protection (DP) and Government Security Classification (GSC) refresher sessions. This training was last delivered in May 2015 and it was reported that the intention is to run the sessions again in November/December this year.

All staff will be required to sign an attendance sheet, two or three "wash up" sessions will be provided for staff that are unable to attend the initial session, after that Line Managers will be expected to deliver the training to their staff.

a36. It was reported that approximately 87% of staff attended the mandatory refresher DP and GSC sessions; the non-attendees included several senior members of staff of Grade 7 and above. We were not provided with evidence that there are any specific corporate KPIs or targets for the completion of training, or that the ISF have ever historically reviewed information assurance related training completion across DBS.

a37. DBS reported that they have had problems obtaining accurate training completion statistics from CSL. The responsibility for ensuring that staff undertake the training and provide a copy of their pass certificates lies with Line Managers.

Recommendation:
a36 and a37. Employees at all levels including senior managers need to be aware of what their roles and responsibilities are, specifically in relation to data protection, information security and their employment at DBS. DBS should ensure this training is mandatory for all staff and senior managers should lead by example. Key Performance Indicators (KPIs) should be agreed and statistics should be produced in order to actively monitor the organisations performance to targets regards the completion of training.

Management response: **Decline**

Action: Our face-to-face sessions are a mandatory requirement as is completion of the annual e-learning. Staff are requested to sign an attendance register at the face-to-face sessions and managers are instructed to obtain sight of the e-learning certificate for internal completion monitoring. Several face-to-face mop up sessions were held and following this the responsibility for delivery of further mop up sessions and the presentation material was transferred to line managers with support from the IGO/DPO where required. Attendance statistics are maintained and as reported 87% completion was achieved, above 80% in the DPO ISG face-to-face sessions was deemed acceptable prior to the responsibility being passed to managers.

a38. The DPO and IGSM have extensive knowledge and experience of both information security and data protection from current and previous roles. Whilst the DPO has a Data Protection qualification the IGSM does not have any formal qualifications in DP but does hold a Certificate in Information Security Management Principles (CISMP) and is a member of the Institute of Information Security Professionals (IISP).

a39. In addition, the DPO and IGSM provide adhoc information security and data protection training to business areas on request. None of this additional training is included in a formal strategic training plan.

Recommendation:
a38 and a39. See Recommendation **a33** and **a34**.

Management response: **Partially accept**

Action: The qualification already held by the IGSM covers the Data Protection principles and is a formal qualification supplemented by IISP membership which requires evidence based experience in Data Protection. This is further being enhanced through the PDR process on an ongoing basis each year through the personal development plan and then progressed through L&D as required. At the time of the audit both the DBS Line Manager and the IGSM had already identified further professional development to include the Data Practitioner Qualification.

The annual e-learning and face-to-face briefings are included in the annual business plans. Individual training/awareness requests from managers are provided by DPO and IGSM as part of the proactive ongoing support provided to the business.

Implementation date & owner: **31/03/2017 WITHHELD**

a40. The Business Support Unit (BSU) provide a tour to new staff making them aware of the risks of tailgating, the importance of securing their workstations and cupboards, and the need to challenge anyone without ID or a

pass. We did not observe any information security awareness materials or reminders for staff processing personal data of their responsibilities anywhere in the building.

Suggestion:
a40. The training and awareness materials on the ICO website could help to maintain a security conscious culture within DBS. The Think Privacy materials/toolkit and Copyright free awareness posters provided by CESG are free to use, DBS would benefit from ordering some publications to use across the organisation.

a41. The HoSaF acts as deputy SIRO and attended the SIRO and IAO training sessions provide by The National Archives (TNA). In addition, the HoSaF attends the Communications Electronics Security Group (CESG) annual information assurance seminar. These roles are also required to complete an additional level on the CSL course.

Suggestion:
a41. Ensure that staff with responsibilities for information governance and data protection, including the SIRO, Deputy SIRO and IAOs, continue to receive specialist training that is refreshed on a periodic basis, and will enable them to identify and resolve information risks effectively. See recommendations **a33** and **a34**.

Access Control – User Access Management

a42. We were provided with policy documents that detail the process to follow for managing user access permissions in relation to starters, movers and leavers and access control for information systems. The policies cover all TCS/DBS employees, contractors and third party suppliers. Although the policies were created/reviewed in June 2015 it appears that they are not yet finalised, approved or distributed to staff and the annual revision date has passed.

Recommendation:
a42. See recommendation **a02**.

Management response: **Partially Accept**

Action: Refer to management response A02.

Implementation date & owner: **31/12/16 WITHHELD**

a43. The HR Staff Departure Procedure (Policy Reference DBS 063) is dated 14 April 2014 and appears to be the current policy. It was due for review in April 2016. The procedure covers voluntary resignation, dismissal, IT accounts, Line and Security Manager responsibilities. The IGSM authorises all access to DBS systems, changes in access and also when staff leave that there access is removed. The policy states that: the staff departure process will be audited by the DBS Security/Audit teams and the Security Manager is responsible for ensuring accounts have been deleted. We were not provided with any evidence that this procedure or any user accounts themselves are audited.

Recommendation:
a43. Introduce regular audits of the movers and leavers process and ensure that accounts/access permissions have been amended or deleted promptly. This will 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.

Management response: **Partially accept**

Action: Audit checks are undertaken on an ad-hoc basis. This has already been included in the scope for the internal assurance framework that is currently under further development to formalise the checks. This will be further reviewed at the implementation of R1.

Implementation date & owner: **31/03/17 WITHHELD**

a44. All IT accounts are suspended and building passes collected when periods of absence exceed 30 calendar days, this includes career breaks, sick Leave or maternity leave.

a45. The DBS IT Support manager and their team have to be SC vetted before being able to administer any accounts. Their role includes providing access to databases; creating new accounts and amending/removing access permissions for movers and leavers.

a46. DBS IT Support utilise a User Role Matrix to allocate appropriate access; the matrix details the role name, function ie description of what the various access/user permissions mean, grade of the role and various Teams :IDM Teams, HUB, OASIS**,** Autobar, Secretariat, Appeals, QA and DRAM.

a47. DBS IT Support must ensure that there is a segregation of duties so that a user is not able to both input and approve permissions. The IT Team and TCS have administrator privileges; monthly reports are produced on approver and inputter roles to ensure that they remain segregated. No issues have been identified to date.

a48. Access to mailboxes, system files, folders and logs is restricted to the relevant team members.

a49. uCRM case records contain the individuals' name, address, date of birth, national insurance number, conviction data, PNC results, summary of case and notes, letters and correspondence.

a50. uCRM does have some role-based restrictions but they are limited (eg. if a user can add a contact record on the system they are not able to bar a person). All uCRM users are able to read all cases irrespective of their role. Records cannot be locked down or access restricted to particular individuals.

a51. A User account request form is completed and authorised before access to the network/uCRM is granted or amended. The form requires three signatures to authorise including the IGSM's.

a52. The IT Database Administrator retains a log of all users' permissions, movers and leavers since 2009. The log records dates, authorisation, amendments, old and new role, disabled accounts and updates.

a53. HR do not always inform IT when someone leaves and notifications from Line Managers in relation to staff changes are inconsistent. There is currently no reconciliation of user access with HR records undertaken.

a54. uCRM has a limited number of user licences; in April 2016 IT discovered that they had almost reached the maximum number of users for the system. They obtained a list of all current staff from HR and found 13 unused uCRM accounts still allocated to staff who had left the organisation or changed roles and no longer required uCRM access.

Recommendation:
a53 and a54. See Recommendation **a43**.

Management response: Partially accept

Action: Ad hoc checks are undertaken at present, however the Assurance Framework is being further developed to formalise these checks. See A43. For clarification when the details in paragraph a54 were verified with our ITSM team they confirmed that of the 13 staff members 12 had moved to other roles internally with only one individual having left the organisation. This will be further reviewed at the implementation of R1.

Implementation date & owner: 31/03/17 WITHHELD

a55. The DBS Barring uCRM system is "air-gapped" from any outside connection and all ports are locked down. A limited number of users have extract and burn privileges to be able to extract information from internal email to the DBS Airgap team. The DBS Airgap team have no access to any data within the uCRM system only email contents. The extracted information is burned to disc, checked that it is appropriate and protectively marked then manually transferred to the POISE system to send on to secure email addresses outside of DBS. Communication between Barring Operations and the wider DBS is undertaken by email which is burned to CD by Airgap and

transmitted by the POISE system and vice versa. For the wider DBS to communicate with Operations Barring the Airgap team burn to disc on the POISE System and manually transfer to the uCRM system to forward on by email.

a56. Sensitive cases that are high profile or likely to attract media interest are handled by a Sensitive Case Officer (SCO), all related casework is additionally protected and accessible only by pre-authorised staff.

a57. All DBS staff have access to the main doors of the building. The only areas which are subject to higher access restrictions are WITHHELD. These areas are restricted to authorised staff. TCS have access to all areas of the building, as they require access to carry out their duties.

a58. A limited number of staff are trained to use the Police National Computer (PNC). The PNC terminal is WITHHELD located in WITHELD and access is restricted to trained PNC users, members of the IT and facilities teams only.

Access Control – User Responsibilities

a59. The TCS Secure Logon Procedures document is the Access Control Procedure for both physical and logical access to ICT systems and data. Access to sensitive DBS assets will be on a need-to-know basis in accordance with job role and with an appropriate level of personnel security control. The policy was approved in June 2015 by TCS but has not been distributed to staff.

a60. The TCS DBS Password Policy document states that the policy owner is the previous SIRO; the Policy was approved in June 2015. This policy covers the minimum standards required in relation to password creation, protection, management and change for standard and privileged user accounts. Staff must treat passwords and/or other access credentials as sensitive information such as a bank PIN. However, as with other TCS policies it has not been disseminated to TCS and DBS staff and passed the review date.

Recommendation:
a59 and a60. See recommendation **a04**.

Management response: **Partially accept**

Action: Refer to Management response a04**.** DBS had already identified the requirement for an uplift as per a02 & a03 response above and the work commenced on this in May 2015. . A conscious decision was taken by DBS not to publish these Policies until R1. Due to a delay in the implementation of R1 DBS reviewed this decision and staff facing policies will be communicated to staff by 31/12/16. Technical policies that current systems are unable to comply with will remain to be published at R1 implementation An example of this is the password policy although uplifted it does not make any changes for staff.

Implementation date & owner: **31/12/16, WITHHELD**

a61. Staff confirmed that the standard password requirements are included in the eLearning. The requirements state that passwords should be complex, including both upper and lowercase letters as well as a number. Users are prompted to change their password regularly and, at the same time, are reminded of the criteria for creating one. Users are told not to write passwords down or share them. WITHELD

Access Control – System and Application

a62. There is a strict process for post arriving in the building. This is overseen by the Facilities team. All items are x-rayed and logged in before they are transferred to COST/OASIS for opening and onward distribution.

a63. Access to paper records identified as sensitive is restricted to the dedicated SCO. The key used to lock the records is stored in WITHHELD. The associated uCRM record will contain sensitive personal data but with minimal details. However due to limitations with the uCRM system it is not possible to restrict user access to the electronic record.

a64. User activity and/or system/data audits are not undertaken.

Recommendation:
a64. See recommendation **a118.**

Management response: Partially Accept

Action: At the time of the audit DBS had already identified this issue and has ensured this has been designed and will be implemented in R1. This is not undertaken currently due to technical constraints with the legacy system but has been included in the design for R1.

Implementation date & owner: In line with R1 delivery plan.

Suppliers Relationships

a65. The DBS, TCS and HO Contract, dated October 2012, sets out new and replacement services for the running of DBS; it was created under the Protection of Freedoms Bill 2012 and the transfer of the functions of the CRB and the ISA on 1 December 2012. Information security requirements, such as right of audit, quality monitoring, staff vetting and training, are included. The contract does not appear to have been reviewed since November 2014 and it is unclear how often the contract is, or should be, subject to review.

Recommendation:
a65. The contract with TCS, HO and DBS must be reviewed and updated to reflect current arrangements and any changes to the agreement. Following on from this, the contract should be agreed and responsibility to ensure it is regularly reviewed assigned to the most appropriate senior manager.

Management response: Decline

Action: The right to assess third party supplier security arrangements is a contractual obligation and a contractual security requirement. Changes to the contract are managed through formal Change Control.

a66. The TCS Supplier Relationships Security Management Policy and Procedures, dated 21 September 2015, include the appropriate information security clauses. The policy has been reviewed by DBS but not yet approved by them or disseminated to the appropriate TCS/DBS staff. We were not provided with any evidence that a PIA was recommended or required to be conducted to allow DBS to assess the third party supplier's information security arrangements.

Recommendation:
a66a. DBS should ensure that third party supplier's information security is assessed as part of a PIA.
a66b. As part of their review of information security policies, see recommendation **a04**, DBS should ensure that the requirement to undertake a PIA to assess third party suppliers' information security is formally included within an appropriate policy.

Management response: **Decline**

Action: The right to assess third party supplier security arrangements is already a contractual obligation and a contractual security requirement which is assured by the Security Assurance Framework and reported at OPSEC.

a67. TNT Business Solutions is the third party provider of off-site storage for DBS records. In January 2015 an audit of the ISO 27001:2013 security controls at TNT, WITHHELD site took place; auditors included the DBS/TCS Accreditor and the IGSM. The objective of the audit was to gain assurance that the business functions and infrastructure being discharged by TNT, in respect of the DBS contract, met the required levels of security and information assurance; and that the provision of Security, Information Assurance, Data Protection and contractual arrangements supported the annual statement of internal controls. The outcome of the audit was described as very good with assurance from the fact that TNT are WITHHELD. Only two minor observations were recorded which relate to improvements by DBS.

a68. The TCS Audit Policy and Procedures, reviewed in November 2015, confirm that TCS's third party suppliers are subjected to an ongoing supplier assurance regime conducted by the TCS Operations Security team. They validate the assurance of the supplier's ISMS, as per the contractual requirements and ISO 27001 standards. There is no approval date for this policy and it has not been disseminated to the appropriate staff.

a69. A services agreement between TCS and Pitney Bowes, dated 30 January 2013, includes information security clauses including staff vetting, right to inspection, audit and monitoring, review the integrity, confidentiality and security of the Data, DPA and FOIA obligations. It is unclear how often this agreement is reviewed or if any audits have been conducted.

Recommendation:
a69. DBS should review this agreement periodically and ensure that it continues to meets their requirements. In addition, compliance checks should be carried out on all contracts and agreements with third parties to ensure that their processing is in compliance with the relevant terms and conditions.

Management response: **Decline**

Action: We already have measures in place to address this. The agreement referred to is a contractual arrangement between TCS and Pitney Bowes and therefore DBS would not review this, this is a TCS responsibility however the obligations contained within the main contract between TCS/DBS mandate that requirements are incorporated within TCS third party sub contracts. There is a supplier assurance framework in place and audits are conducted in line with the framework.

a70. DBS are provided with Certificates of Understanding and Acceptance and DPA Proof of Learning forms from TCS Training and development. They are completed and signed by TCS Call centre staff to confirm that they have read and understood, and agree to comply with, the various TCS/DBS information security policies and procedures.

a71. The Incident Management policies and procedures include the requirement that TCS, third parties and suppliers comply with them. They also detail the procedure to be followed in the event that an incident results in the disciplinary procedure being invoked.

Incident Management

a72. There are a number of policies and procedures that appear to cover Security Incident Management:

- Information Security Incident Management Policy;
- User Security Incident Management Procedure;
- Security Incident Management Procedure.

They do not appear to have been finalised, approved or disseminated to all staff.

Recommendation:
a72. See recommendation **a04**.

Management response: **Partially accept**

Action: Refer to A04

Implementation date & owner: **31/12/16 WITHHELD**

a73. There are duplicate User Security Incident Handling Procedures. Policy (Ref. TCS.03.494 v 2), one is due for review 22 December 2014 and the other is due for review in February 2016. The 2016 copy has the Security Incident Reporting Form attached.

a74. This Policy is the user-facing Security Incident Handling Procedure to assist all TCS/DBS staff in the reporting of security incidents. The flow chart contained within the Policy shows that the form should be completed by the member of staff who should report the incident to their Line Manager immediately. The Line Manager should then report to TCS/DBS security within four hours. The procedure includes incident containment, resolution and lessons learned.

Recommendation:
a73 and a74. DBS should review the User Security Incident Handling Procedure and ensure that it accurately reflects the procedure that staff are expected to follow when reporting all actual and potential security breaches. Once the procedure is finalised staff should be made aware of their responsibilities, what is expected of them and, where the policy and procedure can be accessed.

Management response: **Decline**

Action: All Barring staff were provided with the policy and signed to say they understood. All new staff are taken through high level outline of policy included in induction pack.

a75. Staff confirmed their awareness of a formal documented procedure in relation to information security breaches, incidents and near misses and advised the Auditor that they would report all such events to their Line Manager or IGSM, who would then complete the security incident report form.

a76. However, awareness of the procedure that staff should follow if they discovered a security breach or incident was inconsistent; not all staff could confirm where the policy and/or procedure was stored (ie iGap, horizon/POISE or their team folders), who was responsible for completing the form, how long they should wait before reporting and if there was a list of breach examples that they could refer to.

Recommendation:

a75 and a76. To provide management with evidence that all staff are made aware of their obligations with regard to reporting security incidents, introduce a requirement for staff to confirm that they have read and understood the Policy and Procedure.

Management response: **Decline**

Action: All Barring staff were provided with the policy and signed to say they understood. All new staff are taken through high level outline of policy included in induction pack.

a77. DBS maintain a log of all reported security incidents, breaches and near misses. This is managed by the IGSM and DPO. The security incident report form includes a description of the incident, details of the Line Manager, investigation, identified cause(s) and actions taken; it is sent to the IGSM and DPO who will determine if it is a near miss, incident or breach. Once the investigation is complete a route cause analysis is undertaken. Assurance is provided to the SIRO via the ISF and quarterly reports to the ARC.

a78. DBS operations have secure print facilities; each person has their own unique PIN to allow them to collect their prints. This was introduced as a result of a breach and reduces the likelihood of printed documents getting mixed up and sent to the wrong person.

a79. As a result of an information security breach incident a new internal process has been introduced. A monthly file reconciliation audit takes place which involves checking the location recorded on uCRM and access database (where case file details and contents are recorded) with the contents of the paper records stored in the cabinets. They do not formally report on these audits and to date all files have been accounted for.

a80. In addition a full reconciliation of all off-site records has also been conducted. These actions have resulted in two missing files being found, they had been misfiled.

a81. When a case file cannot be located there is a process whereby all cabinets, pedestals, office desks are thoroughly searched. If any staff member is absent at the time then security will provide access to their pedestal

drawers. No confidential information should be kept in personal desk pedestals. A previous incident involving files being found in a staff pedestal resulted in disciplinary action; following this incident all Team Managers are now accountable for double checking all pedestals and cabinets.

a82. Staff confirmed that they receive regular updates and guidance relating to information security including lessons learned via team briefings or bulletins.

Compliance

a83. There is a Security Monitoring Policy, dated July 2015, which, as with other policies, has yet to be published to staff. This document provides guidance to technical teams in relation to the implementation and ongoing management of the security monitoring solution deployed by TCS for DBS. All systems and applications that collect, store and process citizen data shall be in-scope of security monitoring.

a84. There is an Audit Policy and Procedures document last reviewed in November 2015, which has no approval or distribution date. The audit approach outlined in this document is targeted at TCS Staff, and focuses on the information systems and business processes engaged in the TCS/DBS service delivery.

Recommendation:
a83 and a84. See Recommendation **a04**.

Management response: Partially accept

Action: Refer to Management response A04

Implementation date & owner: 31/12/16 WITHHELD

a85. The TCS Operations Security Assurance regime, once implemented, will include scheduled verification, spot checks and random verification of the systems/components; there will be a rolling programme of monthly

compliance audits. An external ISO 27001:2013 certification audit will be conducted on a yearly basis by an external UKAS accredited organisation.

a86. As a result of an information security breach in 2014 an internal audit was undertaken by the HO and a report was published. Weaknesses were identified in the processes for checking printed material before despatch and validating addresses. A number of controls have been put in place to mitigate the risks identified:

- Pin to Print;
- Letter failsafe check whereby there are two people checking all documents (eg. page numbers, case relevance and spelling errors) before despatch;
- Address validation procedure.

a87. The address validation procedure was introduced due to gaps being identified in the process. DBS have various conflicting information sources including some historical sources. Sources include: DBS records, PNC, Police records and employer information. The new process introduced a combined "are you there" and "occupier letter" template requesting a response from the addressee or occupier to confirm the address before sending any personal information. This new process was disseminated to staff via operations bulletins and is stored on iGap.

a88. The DBS building has a manned reception desk. WITHHELD. The security guards will undertake a series of security checks WITHHELD. They check for clear desks, printers and that cabinets and windows are locked.

a89. If security guards discover an issue involving DBS data they will contact the Facilities Team as they are not permitted to touch case files etc. Any such occurrence will be logged as a security breach.

a90. The clear desk and screen policy is strictly enforced. All paperwork and files from desks must be locked away in cabinets at the end of the day. Keys are stored in key cabinets. The use of mobile phones are prohibited in the confidential area due to the camera facility and security risk, staff can only use them in corridors and kitchen areas.

a91. Each business area has a rota whereby staff are responsible for ensuring that windows are closed, work stations are logged off, screens are switched off, desks are cleared, cabinets and safe are locked, printers are clear, and the WITHHELD is locked at the end of each day. Confirmation of these checks is recorded on an "End of Day Security Check List" record sheet and checked again by a second person. This record sheet is retained and periodic checks are conducted by the IGSM to ensure compliance.

a92. We were advised that DBS IT support is WITHHELD. TCS have the facility to audit user and network activity on cases that have been deemed sensitive/high profile or if someone has declared a conflict of interest. WITHHELD

Recommendation:
a92. See recommendation **a118**.

Management response: Partially Accept

Action: Refer to management response a118

Implementation date & owner: In line with R1 delivery plan.

Operations Security – Operational Procedures and Responsibilities

a93. It was reported that that there are a number of guidance documents which provide detailed breakdowns of key operational security procedures. It was not clear if these documents were produced centrally or locally, within individual teams, and whether they were required to be signed off in the same way as the over-arching policies.

Recommendation:
a93. Clarify the status of operational guidance documents, including staff handbooks and desktop procedures. Consider whether central oversight of such documents would be beneficial, particularly as the new system beds in.

Management response: **Decline**

Action: Prior to the audit all staff and managers had been instructed to only use centrally produced security and Information Management policy and guidance and where directed to destroy any locally held copies.

a94. There is a DBS Security Assurance Framework which outlines how DBS will gain assurance in relation to the security arrangements provided by TCS. It appeared that this framework was mainly geared towards providing assurance once the roll-out of R1 was complete.

Recommendation:
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.

Management response: **Decline**

Action: R1 was not within the scope of the ICO audit and therefore this recommendation is rejected. However DBS will take this recommendation as an observation for the implementation of R1. This is business as usual for DBS. The security assurance framework is embedded in our Operational Security activities which will continue post R1 supplemented by the development of the Internal Assurance Framework.

a95. The DBS Security Assurance Framework states that compliance will be measured against a number of controls which are set out in the Baseline Control Set, included as an appendix to the framework, which are aligned with ISO27001.

Operations Security – Protection from Malware

a96. The TCS Operations Security Policy and Procedures includes a section on controls in place to protect against malicious code. However, it was reported that this policy is not yet in use, as it pertains to the forthcoming R1.

a97. A recently conducted IT Health Check identified a number of issues that were likely to impact upon DBS' ability to protect its systems from malicious code.

a98 - a100. WITHHELD

a101. It was reported that while DBS had elected to tolerate some of the risks identified in the IT Health Check, as it was anticipated that the advent of R1 would address many of them, where such risks would not be addressed by R1 a remediation plan was in place to mitigate them.

Recommendation:
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.**

Management response: Partially Accept

Action: R1 was not within the scope of the ICO audit however DBS will take this recommendation as an observation for the implementation of R1.Accreditation forms part of BAU which includes regular review of any risks with retesting undertaken as part of the IT Healthcheck accreditation regime. As a minimum an Accreditation review is undertaken annually or following a significant change whichever is sooner.

a102. DBS have endpoint controls in place at WITHHELD to the secure network. WITHHELD is in place to protect against malware. Furthermore, USB ports are locked down, as far as possible, to minimise the risk of contamination from unapproved devices.

a103. The WITHHELD that protects the WITHHELD is kept up-to-date with .dat files.

a104. The POISE system, which is internet facing, is operated by the HO and has malware controls in place. The HO provides reports, in relation to information security, to DBS on a regular basis.

a105. The DBS Security Team will assess TCS' performance against the TCS Assurance Framework and Baseline Control Set. This control set includes monthly checks on controls against malicious code.

Operations Security – Backup

a106. The TCS Operations Security Policy and Procedures includes a section on information back-up. This section sets out the systems and applications that must be backed up and supported by a Backup and Restoration Procedure.

Recommendation:
a106. Once R1 is in place, undertake a review to ensure that Backup and Restoration Procedures are in place for all key information systems.

Management response: **Decline**

Action: R1 was not within the scope of the ICO audit and therefore this recommendation is rejected. However DBS will take this recommendation as an observation for the implementation of R1. This is already part of BAU for ITSM for our current operational systems and will continue to be undertaken following the implementation of R1.

a107. TCS undertake incremental back-ups on a WITHHELD with a full-back up WITHHELD. Back-up tapes are stored off-site at WITHHELD.

a108. It was reported that DBS/TCS have not attempted to undertake a system restore from back-up.

Recommendation:
a108. Backups should be regularly tested to ensure that systems can be safely restored.

Management response: **Decline**

Action: At the time of the Audit DBS had already previously identified that it was unable to test back ups and the risk was considered to whether the live system should be used to test the back up. The risk to BAU was considered and the decision taken not to test back ups on the current infrastructure. DBS has ensured this has been built in to the design for R1.

a109. It was reported that there is currently no Disaster Recovery facility, which would allow DBS to set up a temporary site at short notice if they were required to vacate their current premises in an emergency, for the office in Darlington but this will be possible with the R1 system.

Recommendation:
a109. DBS should establish an action plan to be followed in the event that they are required to relocate premises at short notice.

Management response: **Decline**
Action: Disaster Recovery is in place for the disclosure legacy system. The risk for the lack of DR capabilities for the barring legacy system has been reviewed and accepted by the Audit and Risk Committee. Business Continuity Plans are in place for both systems supported by annual testing.

a110. It was reported that the R1 system will have a built in back-up and recovery system.

a111. The DBS Security Team will assess TCS' performance against the TCS Assurance Framework and Baseline Control Set. This control set includes monthly checks on controls around information back-up.

Operations Security – Logging and Monitoring

a112. There is a TCS Security Monitoring Policy in place which outlines the need for proactive protective monitoring. WITHHELD

Recommendation:
a112. Proactive protection monitoring should be carried out in line with the TCS Security Monitoring Policy when R1 is rolled out.

Management response: **Decline**

Action: R1 was not within the scope of the ICO audit and therefore this recommendation is rejected. However DBS will take this recommendation as an observation for the implementation of R1 This is already in the design and is undergoing testing and will be part of the accreditation process. CESG were engaged to provide an independent review of the Security Architecture Design WITHHELD

a113. The Security Monitoring Policy states that TCS will be responsible for the initial configuration and ongoing maintenance of event logging to allow security incidents to be identified and responded to in a timely manner.

a114. The Security Monitoring Policy states that TCS will implement a security monitoring solution to record all system, network and user-related events. Such events will be recorded in sufficient detail to allow the appropriate response and corrective actions to be taken.

a115. The TCS Security Team will develop security monitoring baseline standards which will include details of the events to be logged, the frequency of monitoring reviews and monitoring controls.

a116. TCS will also be responsible for ensuring that third party suppliers implement security monitoring requirements within their own environments. This will be achieved through contractual agreements and a periodic assurance process.

a117. TCS will undertake quarterly audits or compliance checks to ensure that the monitoring is being carried out in line with the policy.

Recommendation:
a117. DBS should also have a 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.

Management response: **Accept**

Action: At the time of the audit DBS had already identified this as an issue and has ensured this is in the design of R1. This risk has previously been tolerated by the SIRO. Due to the delay of R1 a stretch case has been developed which details the risks the legacy systems are carrying and is currently out for formal review before being presented to the SIRO for consideration and sign off of tolerance of the risks. Development of protective monitoring and the establishment of the TCS security operations centre is already included in the Security Architecture Design and development has included the reporting and SOC procedures. The protective monitoring is currently being used to monitor all test activities for R1 with reports being provided to the DBS Accreditor on a weekly basis to review the content and provide input to the monitoring tool tuning. Following R1 monitoring reports will be provided to DBS Operational Security Manager on a weekly basis to ensure the monitoring tool is operating effectively. A copy of the report being produced and developed during the test phases has been included in the Management Response Evidence Pack.

Implementation date & owner: R1 timescales

a118. At present, DBS utilise standard OS logging of user activity on the confidential network, WITHHELD. This was considered to be sufficient to allow the retrospective investigation of most events.

Recommendation:

a118. The WITHHELD continues to represent a risk. DBS should keep the situation 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**.

Management response: **Partially Accept**

Action: At the time of the audit DBS had already identified WITHHELD and an assessment of risk undertaken taking into account WITHHELD and as such does not present the same level of risk. This has been considered and accepted by the SIRO as low risk. If the R1 roll-out is delayed this would form part of a wider risk assessment that would be needed if the situation arises.

Implementation date & owner: **In line with R1 implementation plans**

a119. Email and internet use on the POISE network is monitored by the HO Office. DBS are provided with monthly reports. However, these show little activity as the majority of staff do not use the network on a regular basis.

a120. The TCS Assurance Framework and Baseline Control Set (see finding **a111**) includes monthly checks on audit logging, system use monitoring, and administrator/operator logs.

Operations Security – Technical Vulnerability Management

a121. The TCS Operations Security Policy and Procedures include a section on the management of technical vulnerabilities. This outlines the need for IT Health Checks to be carried out and for those checks to cover application and infrastructure testing.

a122. The most recent IT Health Check was produced in July 2016. It highlighted a number of risks in relation to technical vulnerability management. These included the use of WITHHELD, WITHHELD, WITHHELD and WITHHELD.

Recommendation:
a122. See recommendation **a101.**

Management response: **Decline**

Action: The July 2016 ITHC risk will not be reviewed post R1 as the system they relate to will no longer be operational. However, all the risks rated as High have been considered and mitigated where possible. The new system replacing uCRM is subject to security accreditation before implementation and will be subject to scheduled ITHC as part of BAU.

a123. The IT Health Check recommended that DBS should design, implement and test a patch management solution.

Recommendation:
a123. As recommended in the IT Health Check, undertake to implement a patch management solution to ensure that system and software patches, as well as AV definitions, are identified in a timely manner to allow the necessary testing to be carried out ahead of changes being applied to live systems.

Management response: **Decline**

Action: There is a patch policy and schedule in place which is underpinned by a patch management solution – Shavlik.

a124. The TCS Assurance Framework and Baseline Control Set (see finding **a111**) includes quarterly checks on controls in relation to technical vulnerability monitoring and control.

Operations Security – Network Security Management

a125. DBS Darlington utilises two separate networks. One is the secure network which carries the uCRM system and is not connected to the internet. The other is the POISE network, which is overseen by the HO Office.

a126. There is a TCS Communication Security Policy and Procedures document which sets out that responsibility for maintaining controls to protect the confidentiality and integrity of DBS data passing over internal and external networks rests with the TCS Operations Security Team.

a127. The TCS Operations Security Team are also responsible for maintaining the availability of network services.

a128. The TCS Communication Security Policy and Procedures defines the measures and controls that are in place to protect the network, network services and associated systems.

a129. The TCS Assurance Framework and Baseline Control Set (see finding **a111**) includes WITHHELD checks on network controls and the security of network services.

a130. As detailed earlier, there is WITHHELD. This means that there is limited information about events that may impact upon the integrity of DBS networks.

Recommendation:
a130. See recommendation **a118**.

Management response: Partially accept

Action: At the time of the audit DBS had already identified the lack of PM (see 118) and this is addressed in R1 design. uCRM is not directly connected to any external systems and as such does not present the same level of risk. This has been considered and accepted by the SIRO as low risk. If the R1 roll-out is delayed this would form part of a wider risk assessment that would be needed if the situation arises.

Implementation date & owner: **In line with R1 plans**

Operations Security – Information Transfer

a131. DBS have a number of policies and procedures in relation to the transfer of information, both internally and externally. These include an Internet and Email Policy, an Encryption and Cryptography Policy and a procedure for verifying a caller's identity over the telephone.

a132. The necessary information is sent by email to the Airgap Team. The Airgap Team review the information to ensure that it is in line with DBS policies and that the email address to be used is correct and, where necessary, secure. They will then burn the information onto a CD and manually transfer it onto the POISE network for onward transmission by email. (See finding **a55**.)

a133. The Airgap Team are responsible for carrying out the process outlined at **a47** however, they don't use checklists or similar to check that emails meet the requirements for sending. They rely upon their own expertise.

Recommendation:
a133. While it is recognised that the Airgap process will no longer be necessary once R1 is in place, there is a risk that the current process is not formally defined. DBS should keep the situation under review and, if there are further delays to the roll-out of R1; consider formally documenting the process and the requirements for transmitting information via this process.

Management response: **Decline**

Action: This is under constant review as part of BAU. The process is very clear, if barring staff need to communicate with other staff in DBS or the outside world they have to go through Airgap, this process can not be subverted due to the technical constraint that uCRm is airgapped from any outside connection. Airgap check that the email is appropriately marked and forward on as requested. If emails are not appropriately marked or there is a question where they are to send it to it is referred back to the original sender to confirm it is not sent outside. For individuals outside of DBS and DBS staff outside of Barring to communicate with Barring staff they must send through airgap for them to disseminated in barring as requested.

a134. It was reported that paper versions of case files do not generally leave the building. On rare occasions they may need to be sent to the Liverpool office; in these circumstances they would be hand-delivered by a member of staff.

a135. DBS try to avoid sending records via post, as far as possible. When communicating with local authorities, police forces etc they will utilise secure email wherever possible.

a136. Where it is necessary to correspond via post DBS will utilise recorded or special delivery.

a137. It was reported that DBS have undertaken a great deal of work around address validation. When dealing with referred parties they are often reliant upon the address provided by the referrer; they are, therefore, keen to ensure that this address is correct before sending correspondence.

a138. It was reported that, ideally, DBS would like to be able to utilise DWP/HMRC records to verify addresses, but this would require legislation to achieve.

a139. There are processes in place for sending personal data to referred parties. The intention is to verify that the correct information is being sent to the right party. Below is an example of one such process that was discussed during the audit:

a140. 'Minded To Bar' bundles are sent out to the referred party once a final decision is made by a caseworker. This will consist of the information that was used to arrive at the decision but will be limited to the information that it is necessary and appropriate for the party to see.

a141. There is a double-check process whereby a colleague will check a caseworker's bundle and the redactions that have been made.

a142. Once the casework teams have completed the necessary checks the bundle will be sent to the COST/OASIS team who will check the bundle and log what is being sent out on uCRM. The final bundle will be checked for a number of criteria, including number of pages; these checks are recorded on a 'Fail Safe Sheet'.

a143. The 'Minded To Bar' bundles will then be sent out using the double envelope technique and issued by special delivery.

a144. DBS have a fax machine but it is not connected at present and no staff reported ever using it.

a145. There is no remote or Homeworking facilities for operational staff. Corporate Services staff are able to work remotely via encrypted laptops connected via VPN. This can only connect to POISE and staff with laptops are not capable of connecting to uCRM. RSA tokens are utilised for these remote connections to provide dual factor authentication.

a146. Once a casefile is closed, the manual record is stored on site for three months before being transferred to TNT's secure off-site storage facility in WITHHELD. DBS piggyback on a Ministry of Defence (MoD) contract for off-site storage which allows their records to be stored with a level of security which exceeds strict requirements.

a147. Closed case files are transferred to off-site storage by the Admin Officers in OASIS; all files are logged on an access database which is updated when the location changes so they can be tracked. Once the boxes are full they are security tagged and barcoded with a URN which is recorded on the database. On collection TNT scan the barcode onto their system.

a148. When boxes are collected and delivered a two person check is undertaken on the inventory for both outbound and inbound files. Collection and delivery notes are checked and signed by both the TNT driver and DBS staff member. A DBS colleague will conduct an independent verification and any errors will be detected and resolved. As TNT only have access to boxes and not the contents, any damaged boxes found at TNT will be re-boxed into a larger box and reported to DBS to allow them to check that the contents are correct and secure.

a149. Confidential Waste is managed by PHS Datashred. They supply lockable wheelie bins which are located throughout offices. These are collected and emptied on a weekly basis. Facilities staff observe the on-site destruction process; however it was reported that receipts/destruction certificates are not obtained.

Recommendation:
a149. Ensure that nominated staff are obtaining collection and destruction certificates that correspond with the amount of paper waste or equipment that has been collected and destroyed.

Management response: **Decline**

Action: This is undertaken as part of the Government Framework contract, the destruction is done on site and is witnessed by DBS Facilities or the DBS Security Guard which provides a higher level of assurance than a certificate that will say no of bins shredded.

a150. CDs which are used by the Airgap Team for transferring information between networks are destroyed at the end of each day or when they are full. They are disposed of on-site using a shredder. The resulting waste products are collected by the same company who handle confidential paper waste.

a151. The DBS Security Team will assess TCS' performance against the TCS Assurance Framework and Baseline Control Set. This control set includes monthly checks on physical perimeter security and entry controls, internal physical security, and security of equipment off premises. The control set includes quarterly checks on controls in relation to the secure disposal of equipment. The control set includes biannual checks on controls around information exchange policies and agreements, the use of electronic messaging, message integrity, reporting of information security events.

7.2 Scope: Data sharing. The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

Risk: The failure to design and operate appropriate data sharing controls is likely to contravene the principles of the Data Protection Act 1998, which may result in regulatory action, reputational damage to the organisation and damage or distress for those individuals who are the subject of the data.

Informed Decision Making

b01. There are a number of legal gateways which allow DBS to disclose sensitive personal information to third parties. The significant legislation which permits the DBS to disclose barring information to Supervisory Authorities (SA) and Keepers of Registers (KoR) is the Safeguarding Vulnerable Groups Act 2006 (SVGA) and the Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 (SVGA).

b02. The DBS Data Sharing Catalogue provides an overview of the data the DBS shares with third party organisations and the legislation in place which legally permits the sharing of information.

b03. It was reported that the decision to share DBS barring data is discussed and approved at a senior management level. However, the IGSM and the DPO are not involved in the initial decision making discussions. There was uncertainty regarding the data sharing decision making process for disclosure information.

Recommendation:
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.
Management response: **Partially Accept**

Action: At the time of this audit DBS had previously identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and actively reviewing the Data Sharing process and templates and governance arrangements.

Implementation date & owner: **WITHHELD 31/01/17**

b04. Where a decision has been made by senior management to proceed with a data sharing proposal, the IGSM is contacted to consider the data protection implications and provide recommendations.

Recommendation:
b04. Recommendations or comments provided by the IGSM in relation to the data sharing project should be formally recorded. See recommendation **b03b**.

Management response: **Partially Accept**

Action: At the time of this audit DBS had previously identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements. Advice is currently formally documented in emails and on comments sheets sent out through the formal document reviewing process i.e. MoU, PIA.

Implementation date & owner: **WITHHELD 31/01/17**

b05. Once all reviews have been conducted, and recommendations or comments have been provided to the business area for consideration, the SIRO is responsible for approving the information sharing. No evidence was provided to support that the final sign off is formally documented.

Recommendation:
b05. Ensure that the final sign off provided by the SIRO is formally documented. See recommendation **b03b.**

Management response: **Partially Accept**

Action: At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was in place and reviewing the Data Sharing process and templates and governance arrangements where SIRO sign off has been required this has been documented in an email by the SIRO which is saved in the CFP.

Implementation date & owner: **WITHHELD 31/01/17**

b06. There is no policy or procedure in place to clearly set out the data sharing process or the processes to be followed for both disclosure and barring information.

Recommendation:
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 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.

Management response: **Accept**

Action: At the time of this audit DBS had previously identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and actively reviewing the Data Sharing process and templates and governance arrangements that will be rolled out across the whole of DBS.

Implementation date & owner: **WITHHELD 31/01/17**

b07. No specialised data sharing training is provided to individuals involved in making decisions regarding data sharing. The IGSM has not received any specialised training for their current role and is waiting to attend a data protection course.

Recommendation:
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**.

Management response: **Partially Accept**

Action: Within our barring function we currently undertake several job role specific training which incorporates data handling, redaction and data sharing as appropriate to the role. At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements.

Implementation date & owner: **WITHHELD 31/12/16**

Assessing Legality, Risks and Benefits (PIA)

b08. There is no policy in place requiring a PIA to be conducted for new projects in which personal data is shared or for existing data sharing projects where a significant change is involved. The DBS are currently referring to the HO PIA policy.

Recommendation:
b08. See recommendation **a24**, the requirement to conduct a PIA involving data sharing, should be documented in a DBS policy.

Management response: **Partially Accept**

Action: The policy that DBS follow with regard to PIA is the Home Office Policy as it was reviewed and found fit for DBS purposes. At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process, templates and governance arrangements incorporated into a tool kit. See a24.

Implementation date & owner: **WITHHELD 31/01/17**

b09. It was reported that PIAs are conducted for all new projects involving data sharing. However, PIAs were not carried out in the past and, as a result; PIAs have not been carried out for some data sharing projects which are already in place. Auditors were provided with a sample of PIAs carried out by the DBS; some of the examples that were provided were outdated and had not been revisited since the formation of DBS.

Recommendation:
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.

Management response: **Partially Accept**

Action: The policy that DBS follow with regard to PIA is the Home Office Policy as it was reviewed and found fit for DBS purposes PIAs are currently reviewed when there is a change to the data being shared and also in the event there was no original PIA undertaken pre Cabinet Office mandate a PIA is developed to address the original data share and incorporate the change. At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements of which PIA is incorporated.

Implementation date & owner: **WITHHELD 31/12/16**

b10. The PIAs carried out by the DBS include an introduction, an outline of any legal basis for disclosure, exemptions that may apply, data handling, privacy law and data protection compliance checks, purpose and a summary of the privacy risks and mitigations identified.

b11. It was reported that business areas involved in a data sharing initiative are responsible for conducting a PIA. Documentation recording the outcome of any PIAs that are carried out is held by the individual business area involved.

Recommendation:
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.

Management response: **Partially Accept**

Action: The IG team are already involved in reviewing PIAs and providing documented comments on the review through the formal document review process. At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements. The IG team are already involved in reviewing PIAs.

Implementation date & owner: **WITHHELD 31/12/16**

b12. PIAs undergo a review by key stakeholders, including the SIRO, Legal team and Policy team. The IGSM is also responsible for reviewing PIAs relating to the sharing of barring information. Where the sharing involves disclosure data, the DPO is responsible for reviewing the PIA. Comments as a result of the review are not documented on the PIA.

Recommendation:
b12. Comments provided by key stakeholders, as a result of the PIA review, should be formally documented, on the PIA documentation, for audit and monitoring purposes.

Management response: **Decline**

Action: PIA are issued for both internal and external review through the standard document review process. Comments are formally recorded and responded to by the author of the document.

b13. The SIRO has overall responsibility for signing off PIAs.

b14. DBS does not currently maintain a log of all PIAs that are carried out and their outcomes.

Recommendation:
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.

Management response: **Accept**

Action: At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had obtained an additional resource which was in place and reviewing the Data Sharing process and templates and governance arrangements.

Implementation date & owner: **WITHHELD 31/01/17**

Information Sharing Agreements and Logs

b15. DBS does not have a formal policy which sets out the circumstances in which an information sharing agreement (ISA) is required to be put in place.

Recommendation:
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.

Management response: **Accept**

Action:

Implementation date & owner: **WITHHELD 31/12/16**

b16. There are information sharing agreements (ISA) in place between KoRs and SAs receiving barred information and DBS. The agreement is in the form of a Memorandum of Understanding (MOU).

b17. The MOUs which are in place, set out the purpose of the contract, the roles and functions of the two parties, and the information flows between the parties. The information flows detail the legal basis under which barred information can be shared between parties.

b18. The MOUs that were reviewed during the audit were supported by additional information and guidance for KoRs and SAs within the Appendices.

b19. Information sharing MOUs are not based on a standard template. Business areas are responsible for drafting their own MOUs.

Recommendation:
b19. Create a standardised MOU for information sharing to ensure that MOUs are consistent across the DBS.

Management response: **Partially Accept**

Action: At the time of this audit there was a standard barring MoU template. DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements to ensure a DBS wide process and template are put in place.

Implementation date & owner: **WITHHELD 31/01/17**

b20. It was reported that there are also MOUs in place between the DBS and third parties receiving disclosure information. As Disclosure was outside the scope no evidence of MOUs for disclosure information was provided to ICO Auditors. To guarantee consistency, it would be good practice to ensure that information sharing MOUs across DBS are based on the standard template.

b21. Once drafted, MOUs are reviewed by key stakeholders, this includes the IGSM and DPO; recommendations and comments resulting from the review are not formally documented.

Recommendation:
b21. Formally document MOU reviews carried out by key stakeholders.

Management response: Decline

Action: MoUs are issued for both internal and external review through the standard document review process. Comments are formally recorded and responded to by the author of the document.

b22. The Head of the business area is responsible for signing MOUs on behalf of the DBS. MOUs are signed by the Chief Inspector or Chief Executive of the third party organisation entering into an ISA with the DBS.

b23. Information sharing MOUs are held by the business area responsible for the ISA. It was reported that the MOUs should undergo a review every 12 months and this review period is documented in the MOUs. The team responsible for reviewing contracts has not been decided.

Recommendation:
b23. All information sharing MOUs should be held centrally by a nominated department. This department should take responsibility for the oversight process and for regularly reviewing MOUs, in conjunction with the necessary business area.

Management response: Decline

Action: At the time of this audit all Barring MoUs were held centrally previously by the SRM team that have been incorporated into the Comms team.

b24. A contract register is maintained, by the DBS, which details all of the contracts that are currently in place. The register details the start and end date, description of type of contract and comments. Auditors were also

provided with an MOU status for the sharing of barring information. This documents the KoRs or SAs that the MOU is with, the date that the MOU was signed and the scheduled review date. However, a number of contracts have not been signed and review dates on certain MOUs have been flagged as overdue. A log specifically detailing all of the information sharing MOUs in place is not maintained.

Recommendation:
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.

Management response: **Partially Accept**

Action: At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements.

Implementation date & owner: **WITHHELD 31/12/16**

b25. Information Sharing MOUs do not include the right for DBS to audit third party organisations that are receiving DBS data. Assurance is not sought by the DBS to confirm that third parties are complying with the terms of the information sharing MOU.

Recommendation:
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.

Management response: **Partially Accept**

Action: At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had obtained an additional resource which was in place and reviewing the Data Sharing process and templates and governance arrangements

Implementation date & owner: **WITHHELD 31/12/16**

Security

b26. DBS barring information is shared with third parties by email and post. Information disclosed by email must be appropriately marked, in line with the GSC guidelines, and sent to a secure email address such as GSI or PNN. Information sent electronically is sent out via the Airgap Team.
b27. Barring information intended to be sent by post must be sealed into two envelopes and sent by special or recorded delivery.

b28. Before postal mail is sent, it must undergo a letter failsafe check to ensure that all postal correspondence is sent to the correct organisation at the correct address.

b29. To carry out a letter failsafe check staff are required to complete a failsafe template which provides details of the letter the individual intends to send. The number of sheets that are to be sent should also be recorded on the proforma and the member of staff should sign to confirm these details. Once completed, a second member of staff must sign to confirm that the name and address is the same as printed on the letter, the number of pages is correct and the letter has been sealed into two envelopes. This process is documented in the Letter Failsafe Guidance.

b30. Guidance on how to send information when responding to a disclosure request is included in the desk instructions provided to staff. Guidance on how to protectively mark information is detailed in the DBS Information Classification and Media Handling Policy.

b31. Information sharing MOUs that were provided to Auditors did not specifically set out the arrangements under which DBS data would be shared with the third party organisation receiving the information.

Recommendation:
b31. Review information sharing MOUs to include arrangements as to how the data will be shared with the third party.

Management response: **Partially Accept**

Action: : At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements.

Implementation date & owner: **WITHHELD 31/12/16**

b32. Security and Audit Assurance information is included in the appendix of information sharing MOUs. This suggests that the third party organisation receiving DBS data nominates a DBS Data Guardian. The role of the Data Guardian is to take responsibility for the security of DBS data and to ensure that staff are aware of their responsibilities when handling data. However, no checks are undertaken to gain assurance that this requirement is complied with.

Recommendation:
b32. See recommendation **b25a**.

Management response: **Partially Accept**

Action: At the time of this audit DBS had already identified gaps in Data Sharing arrangements and had recruited an additional resource which was already in place and reviewing the Data Sharing process and templates and governance arrangements.

Implementation date & owner: **WITHHELD 31/12/16**

b33. Access restrictions to DBS data have not been included in the information sharing MOUs.

Recommendation:
b33. Ensure that MOUs include access restrictions to DBS data that is shared with third parties. Access should be restricted to authorised personnel within each organisation based on purpose for disclosure and business need.

Management response: **Decline**

Action: Appendix 1: Security and Audit Assurance contained within the MoUs state that access to data must be confined to those with specific authority to view the data on a need to know basis.

b34. Information sharing MOUs do not specifically include the requirement to report security incidents to the DBS, or the process to follow if a security incident has occurred. It was reported that the nominated DBS Data Guardian has the responsibility to report security incidents to the IGSM. No security incidents have been reported to DBS to date; however, if reported, the IGSM is responsible for carrying out an investigation in accordance with the Security Incident Handling Procedure.

Recommendation:
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.

Management response: **Decline**

Action: At the time of the audit the requirement to report incidents was already included in the Security annex and it will be incorporated into the new standard template.

b35. For any internal security breaches, staff are advised to report the breach to their Line Manager, who are responsible for reporting the security breach to the IGSM.

Disclosures

b36. Administrator Officers (AO) and Executive Officers (EO) are responsible for handling information disclosure requests from third parties such as the Police, National Offender Management Service (NOMs), National College for Teaching and Learning (NCTL) and Local Authorities. The legal basis to disclose barring information to third parties is primarily permitted under the SVGA and SVGO.

b37. Third parties requiring barring information from the DBS must submit a request in writing. The request should clearly state the purpose for the request and the legislation that they are requesting the information under. For disclosure requests submitted by Police, all such requests must be countersigned by a Sergeant.

b38. Where a valid request for an individual's barred status is received, the AOs and EOs are responsible for conducting a search on the uCRM system to identify if a particular individual is barred. Searches are conducted by entering the name, date of birth and postal address of individual.

b39. In specific cases, the DBS has the discretion to disclose further information in relation to the bar. This would be in circumstances where the third party has a legitimate interest, or where a regulated activity is involved and the further information is relevant to those functions. EOs are responsible for handling these particular disclosure requests.

b40. The DBS can also release a barred status to prospective or current employers. Prospective employers are required to state the reason for the request. No further evidence is requested from the third party to evidence that the particular individual has applied for a particular position within the organisation.

Recommendation:
b40. When handling barred status request from prospective employers, the DBS should take further steps to request evidence to support that the particular individual under enquiry, has applied for a position within the organisation.

Management response: **Decline**
Action: At the time of the audit DBS has a rigorous process in place to deal with legitimate interest queries in that requests are made through official secure email addresses or on letter headed paper in which it states the reason for the request i.e. they are making or have made a job offer and are awaiting a DBS check. Letters that look suspicious or do not state a reason for the request are googled to identify if they are a genuine company and then further information is requested before any response is made. Staff are trained and are subject to 100% check until they are signed off at which time they will then be subject to 10% QA check.

b41. A log of all disclosure requests received by the DBS is maintained by the departments responsible for dealing with requests. The log details the agency requesting the information, the date of request, reference number, who the request was actioned by, the date the request was sent, any relevant comments and the recorded or special delivery tracking number.

b42. Where there is a specific barring case on the uCRM system, it was reported that a note would be recorded on the individual case file; the note records that a request has been received, and how it was responded to. It was unclear if a note is recorded on the individual case file for all types of disclosure requests received by the DBS.

Recommendation:

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.

Management response: **Partially accept**

Action: The request and response is placed on the file. DBS will review to include the legal basis in all cases is documented.

Implementation date & owner: **WITHHELD 31/03/17**

b43. DBS also proactively releases information. Where an individual has applied for a disclosure certificate, the disclosure area is responsible for enquiring if the individual is barred. Where a breach of bar is identified, the PROMPT team are responsible for gathering information and creating evidence packs. The information is disclosed to the Police force responsible for the overall investigation and the force is notified that there has been a breach of the bar.

b44. Staff responsible for handling information disclosure requests are provided with detailed desk instructions. The instructions explain the legal basis for disclosure and the process to follow when dealing with particular requests.

b45. For barring requests, staff are provided with the 'Am I/Are they on the list' guidance, which is supported by 'a Legitimate Interest' guidance. This guidance is designed to assist staff in deciding whether there is a legitimate interest to release the data to the third party.

b46. Desk Instructions and additional guidance are made available to staff through the staff intranet 'iGap'. Where additional tailored advice is required on an information disclosure request, it was reported that staff would contact the IGSM or the DBS Legal Team.

b47. Responses to information disclosure requests are not authorised by a senior member of staff before they are released.

Recommendation:
b47. Ensure that all information disclosure requests are signed off by a senior member of the team. The sign off should be documented for monitoring purposes.

Management response: **Decline**

Action: There is a defined process that has been agreed and staff are subject to 100% check until they are signed off and then a 10% QA is applied. The process has been reviewed and deemed appropriate to the level of risk.

b48. Quality Assurance (QA) checks are carried out on the information disclosure requests handled by AOs and EOs. For new members of staff, all information disclosure requests are checked until the new starter is signed off by a Manager. For all information disclosure requests responded to by the department, a dip sample of 10% is quality assured.

b49. QA checks carried out are recorded on a QA checklist and provided to the DBS Casework Assurance and Improvements Team (CAIT) who are responsible for monitoring QA checks completed by departments.

b50. Staff responsible for dealing with information disclosure requests are provided with desk-side training with the use of the desk instructions. It was reported that Managers are responsible for logging the training received on a training record. No formalised data sharing training has been provided to staff making informed decisions about whether to disclose personal information to a third party. There was a lack of awareness amongst some staff interviewed regarding the legislation that permitted the DBS to release data to a third party.

Recommendation:

b50a. Staff responsible for dealing with information disclosure requests should be provided with specialised data sharing training. The training should cover information on the legislation which permits the DBS to disclose information to a third party and how to handle data sharing requests. See recommendation **a33**, **a34** and **b07**.

b50b. Refresher training should be provided to staff responsible for dealing with disclosure requests on an annual basis.

Management response: Decline

Action: Any role that involves Data sharing receives specialist at desk training and are subject to 100% check until they are signed off and then 10% QA is applied. Periodic reminders are issued to all staff.

7.3 The agreed actions will be subject to follow up to establish whether they have been implemented.

7.4 Any queries regarding this report should be directed to WITHHELD, Engagement Lead Auditor, ICO Good Practice.

7.5 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures.