CBSL

ICT Review – ICT Management Controls

British Transport Police

Not Protectively Marked

FINAL

August 2012

2012/13

Review of the ICT Management Controls

- EXECUTIVE SUMMARY -

INTRODUCTION

1. We have carried out a review of the ICT Management Controls arrangements within the Force for the British Transport Police. The review was carried out in July 2012 and was part of the planned internal audit work for 2012/13.

SUMMARY

2. One Key Risk Control Objective was tested and based on the findings from this work an overall evaluation of the overall adequacy of the internal controls was established (figure 1 below).

Figure 1 - Evaluations of the Effectiveness of the Internal Controls

Evaluation
Reasonable Assurance

KEY FINDINGS

3. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. Recommendations for improvements should be assessed by the Authority for their full impact before they are implemented. The priorities of the recommendations are summarised below (figure 2):

Figure 2 - Summary of Priorities of Recommendations

High	Medium	Low	Operational
1	4	4	-

RELEASE OF REPORT

4. The table below sets out the history of this report.

Date draft report issued:	20th July 2012
Date management responses recd:	3rd August 2012
Date final report issued:	6th August 2012

MANAGEMENT ACTION PLAN

PRIORITY 1, 2 AND 3 RECOMMENDATIONS

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	The Force not being able to function due to the irrecoverable loss of critical data.	A new Disaster Recovery (DR) centre has been put in place in Birmingham but no full DR testing has yet taken place. It is understood that significant testing on the recovery of individual servers has taken place as part of the implementation of the DR centre. Full DR testing has been postponed owing to the 2012 Olympics and is expected to be undertaken at a later date. This should be undertaken as soon as reasonably possible.	Ensure a full documented Disaster Recovery test is performed to ensure data and systems can be restored as expected.	1	*Fully documented failover and failback to take place post-Olympics. Date of failover provisionally set for Oct 7, and failback for Oct 21.*	*31/10/2012*	*Head of IS&BS*
1	The IT management arrangements are not carried out in a duly authorised manner which may	The Head of Information Services and Business Support has documented an interim Information Services Strategy for the period 2010/11 to 2012/13. The Strategy	The Interim Information Services Strategy be reviewed to ensure any assumptions made in the existing document meet with	2	*The existing strategy has been reviewed and still meets business aims and the requirements of the Government ICT Strategy and DfT restrictions. The IS Strategy refresh*	*31/03/2013*	*Head of IS&BS*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
	lead to financial loss due to an absence of direction and to a lack of accountability.	makes assumptions on the business aims for this period in lieu of BTP's strategic plan (for 2011/12 to 2013/14). Given this, the Strategy should be reviewed to ensure actual business aims are being met. The review should also incorporate the requirements of the Government ICT Strategy and any DFT restrictions.	actual business aims and the requirements of the Government ICT Strategy and DFT restrictions.		*process has now commenced to create a new 3-year strategy to run from April 2013.* *Draft ICT strategy to be prepared by Feb 22 2013, with signoff by SCT to be achieved by 20 March 2013.*		
3	The Force not being able to function due to the irrecoverable loss of critical data.	The backup regime is currently not documented but a member of staff has been tasked with this.	The backup arrangements be documented to ensure the arrangements in place are adequate for recovery purposes.	2	*The backup arrangements are fully operational and meet best practice. Documentation is being updated to reflect current practice.*	*30 Sept 2012*	*Head of IS&BS*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
6	Information assets being lost or stolen, which could breach confidentiality.	Laptops are configured for the use by two persons maximum and would have to be reconfigured to use by other staff. Laptops are signed out on "Syops" forms and a record is maintained. It is noted that on previous audits that some equipment proved difficult to locate such as mobile phones (which are also on the Syops forms) and therefore it is suggested that a sample check of mobile equipment be undertaken periodically.	Regular sample checks be undertaken to ensure equipment registers are accurately maintained.	2	*Sample checks will be undertaken, commencing after the Olympic period.* *All Areas to produce lists of mobile phone and laptop assets, by named user, by 31 Oct 2012. All instances of mobile phones needing international dialling to be verified against business need, and removed where not specifically approved.*	*31 Oct 2012 and annually thereafter*	*Head of IS&BS*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
9	The Authority suffering legal action or adverse publicity due to the use of unlicensed software.	In response to the Microsoft License audit, the IT function is currently preparing a report of all software installations across the corporate network using Microsoft's SCCM (System Centre Configuration Manager) to extrapolate the information electronically for all software vendors from connected machines. Once the report is complete it will be compared to the licenses recorded in the CMDB to ensure compliance has been maintained.	Ensure that a full license reconciliation is undertaken once the SCCM report has been completed.	2	*The SCCM system has been configured to work across the new WAN and detect all machines on the network. An initial SCCM report was completed on 25 July, giving details of all desktops across the network, by Area, with operating system status (including Service Pack update status), make, model and serial number. This will allow us to begin the process of reconciling software licensing across the estate.* *To be completed by Ross Powell (IS&BS), by 30 Nov 2012.*	*30/11/2012*	*Head of IS&BS*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	IT purchasing is not conducted in line with the IT Strategic plan.	Monthly meetings between Finance and the Head of Information Services and Business Support take place where budgets and spending figures are discussed and checked. The Head of Information Services and Business Support has intimated that the budgetary reporting from Finance could be improved by using "Business Objects" reporting software which would allow budget holders to electronically drill down into detailed records.	Consideration be given to the development of electronic reporting for budget holders to enable a more accurate approach to monthly reconciliation.	3	*IT purchasing is conducted in line with the IT Strategic Plan. All purchases are approved by the Head of Dept or CTO, both of whom understand the strategic plan in detail. Better reporting is still needed; discussions will be scheduled with the Head of Finance to see if this can be arranged.* *Meeting arranged for 13 Aug 2012. The controls agreed with Finance will be overseen by the Technology Board which commences on 7th September 2012 and meets monthly thereafter.*	*31/10/2012*	*Head of IS&BS / Head of Finance*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
5	IT purchasing is not conducted in line with the IT Strategic plan.	It is understood that projects are not given their own budget codes to book equipment and services to. This makes project costing difficult to monitor and the Head of Information Services and Business Support has indicated that he has been specifically instructed to not keep his own records for purchasing.	Consideration be given to providing temporary budget codes for projects to enable accurate costing and reconciliation against agreed budgets.	3	*IT purchasing is conducted in line with the IT Strategic Plan. All purchases are approved by the Head of Dept or CTO, both of whom understand the strategic plan in detail. It should however be standard practice that major projects should be given their own budget codes to ensure that there is no confusion between budgets or spend on them and any other IT budgets or spend. Head of IS&BS will liaise with Head of Finance to ensure that this is standard practice going forward.* *Meeting arranged for 6 Aug 2012, and processes and controls agreed to be overseen by the Technology Board.*	*31/10/2012*	*Head of IS&BS / Head of Finance*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
7	Information assets being lost or stolen, which could breach confidentiality.	It is understood that there is no co-ordinated incentive within FHQ to identify and return redundant equipment which could be recycled for use elsewhere rather than having to purchase new equipment.	An internal equipment usage audit be undertaken to identify under-utilised equipment for redistribution.	3	*There is no risk to confidentiality if information assets are lost or stolen, as mobile assets (laptops, Blackberries etc) are encrypted to the approved standards.* *All areas to produce lists of assets (other than mobile phones/latops – see above) by location and user, to verify that assets are needed, by 30 Nov 2012. Unwanted assets to be reported to IS&BS for redistribution.*	*30/11/2012*	*Head of IS&BS*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

Rec.	Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
8	Inappropriate use of email and Internet facilities bring the Force into disrepute.	Several emails were checked by Internal Audit and it is noted that there are several different signature styles in use. Consideration should be given to defining and promoting a standard email signature to ensure outbound email communications have a professional look to them.	Consideration be given to formalising email signatures to ensure all outbound communications look professional.	3	*There is an existing SOP that covers the use of Computers and Comms equipment, and covers inappropriate use.* *The use of standard signature styles is not covered. IS&BS will work with the Force Media Manager to explore whether an automated email signature template can be created for all BTP staff.*	*30/9/12*	*Head of IS&BS and Head of Media*

PRIORITY GRADINGS

1	URGENT	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud.
2	IMPORTANT	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money.
3	ROUTINE	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure.

OPERATIONAL EFFECTIVENESS MATTERS

Ref	Item	Management Comments
	There are no Operational Effectiveness Matters.	

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures, rather than on a one-by-one basis

- DETAILED REPORT -

SCOPE AND LIMITATIONS OF THE REVIEW

5. The review considers the arrangements for: access security; back up retention periods; email/ internet policy & enforcement; licence monitoring, upgrade controls and protocols for communicating with third parties. The scope of the review does not include consideration of the training needs; or the appropriateness of file sharing.

6. The review has been carried out by TIAA Ltd as the nominated sub-contractor of Capita Business Services Ltd ('CBSL'). CBSL is the arm through which Sector's non-FSA regulated services, including the former Sector Business Assurance, are delivered. The limitations and the responsibilities of management in regard to this review are set out in the Annual Plan.

7. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. CBSL and TIAA neither owe nor accept any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

ASSESSMENT OF THE KEY RISK CONTROLS

8. This review identified and tested the controls that are being operated by the Force and an assessment of the combined effectiveness of the controls in mitigating the key control risks is provided. The assessments, which accord with those used by the Department for Transport, are:

Full	Systems of corporate governance, risk management and internal control are fully established, documented and working effectively
Substantial	Systems of corporate governance, risk management and internal control arrangements are well established and working effectively. Very minor control weaknesses have been identified in a maximum of one or two discrete areas.
Reasonable	Systems of corporate governance, risk management and internal control arrangements are generally established and effective, with some minor weaknesses or gaps identified.

Partial	Systems of corporate governance, risk management and internal control are present and operating effectively except for some areas where material weaknesses or significant deficiencies have been identified, aspects of the control arrangements need documenting, or evidence does not exist to demonstrate effective operation.
None	Systems of corporate governance, risk management and internal control are poorly developed or non-existent or major levels of non-compliance or non-conformance have been identified. Control arrangements are not adequately documented, or evidence does not exist to demonstrate effective operation.

MATERIALITY

9. British Transport Police utilise technology for day to day operations. A framework of Standard Operating Procedures is in place to support daily operations which are available to staff through the Intranet. A number of new projects have been implemented since the last review which have improved efficiencies and improved network security. These projects have been defined within an Interim Strategic Plan which is the current driver for change.

AUDIT FINDINGS

Key Risk	Failure to direct the process through approved policy & procedures and/or losses arising from unauthorised action.
Key Risk Controls	Arrangements in place for the process provide for direction through established policies, procedures and provide for safeguarding the organisation's assets and interests from avoidable losses.
Evaluation	**Reasonable Assurance**

10. The following matters were identified in reviewing the Key Risk Control:

Risk: The IT management arrangements are not carried out in a duly authorised manner which may lead to financial loss due to an absence of direction and to a lack of accountability.

10.1 The Head of Information Services and Business Support has documented an interim Information Services Strategy for the period 2010/11 to 2012/13. The Strategy makes assumptions on the business aims for this period in lieu of BTP's strategic plan (for 2011/12 to 2013/14). Given this, the Strategy should be reviewed to ensure actual business aims are being met. The review should also incorporate the requirements of the Government ICT Strategy and any DFT restrictions.

Recommendation: 1	Priority: 2
The Interim Information Services Strategy be reviewed to ensure any assumptions made in the existing document meet with actual business aims and the requirements of the Government ICT Strategy and DFT restrictions.	

10.2 The Strategy is supported by five separate strategies as detailed below and are included within the documented Interim Strategy:

- The Information Management (IM) Strategy
- The Information Systems (IS) Strategy
- The Information Technology (IT) Strategy
- The Service Management Strategy
- The Governance Strategy

10.3 In support of the Strategy is an implementation plan with guide dates for particular projects. It is noted that during the audit, discussions had taken place requiring the Head of Information Services and Business Support to provide detailed business case information for each of the projects to be undertaken, even for those already detailed within the approved Strategy.

10.4 There is a Force Information Security Policy in place dated June 2011. The document owner is the Head of Professional Standards Department and is next due for review in June 2014. The Policy details the general responsibilities with regard to the security of paper based and electronically stored information. The FISP and Standard Operating Procedures are all available through the forces intranet.

10.5 In addition to the FISP there are number of Standard Operating Procedures which include Security of buildings, rooms and containers, Change Control, Portable Data Storage Devices, Remote Access, Laptops, Identity cards and Passwords. These are available to staff through the intranet.

10.6 The IT Service delivery team is split into several departments:

- Service Desk
- Service Management
- Networks
- Communications

- Desktop Application Mobile & Server support
- Information Management

Each of the areas above has a manager who reports to the Head of Information Services and Business Support. The Head of Information Services and Business Support has overall responsibility for IT service delivery and reports to the Deputy Chief Constable. Each member of IT staff has a documented job role which details their responsibilities and accountability.

10.7 There is a documented Service Level Agreement in place for IT service delivery which is available to all staff via the Intranet. Monthly reports are provided to senior management documenting achievement against the agreed Key Performance Indicators.

10.8 Requests for new network user accounts are initiated by the HR team. A form is completed and sent to the Technology Service Desk. A service request is then recorded within the ICCM Service Desk software for action. It is understood that the process is known to the relevant service desk staff but is not documented. A new system is anticipated for the future. This new system will use a data feed from the HR system to track employees, create, close and amend accounts and access permissions as required utilising Microsoft's FIM software. Users will use then utilise two-factor authentication in the form of username and password in conjunction with chip and PIN. The chip and PIN cards will also manage door access Force-wide. It is anticipated that the system will be intelligent enough to check that the user is logging onto to desktops that are in the same building that they have accessed.

Risk: The Force not being able to function due to the irrecoverable loss of critical data.

10.9 A new Disaster Recovery (DR) centre has been put in place in Birmingham but no full DR testing has yet taken place. It is understood that significant testing on the recovery of individual servers has taken place as part of the implementation of the DR centre. Full DR testing has been postponed owing to the 2012 Olympics and is expected to be undertaken at a later date. This should be undertaken as soon as reasonably possible.

Recommendation: 2	Priority: 1
Ensure a full documented Disaster Recovery test is performed to ensure data and systems can be restored as expected.	

10.10 Regular daily backups are made to tape at the Camden HQ site. Force data is also replicated to a DR site in Birmingham in real-time ensuring that data availability is 24/7.

10.11 The backup regime is currently not documented but a member of staff has been tasked with this. It is understood that the following arrangements are in place:

- daily incremental saves (Monday to Thursday including Bank Holidays)
- weekly full saves (the first 3 or 4 Fridays each month)
- monthly (every last Friday each month)
- annually (in December)
- tapes are stored in a fireproof safe in the basement at Camden HQ.

Recommendation: 3	Priority: 2
The backup arrangements be documented to ensure the arrangements in place are adequate for recovery purposes.	

10.12 Local servers in Area offices are backed up daily using Backup-Exec and a local member of staff has responsibility for management of the tapes. It is understood that now that the new WAN project has been completed that these sites will begin to backup across the WAN to a central location, thus removing the requirement for local tape management.

10.13 There is a change management process in place to ensure changes to network settings, configuration and security are undertaken in a controlled manner and is managed through the service desk software.

10.14 There is a Change Advisory Board in place to discuss the arrangements for individual changes raised through the service desk. The actions that have arisen from the meetings are emailed to those involved to implement the relevant changes.

Risk IT purchasing is not conducted in line with the IT Strategic plan.

10.15 New suppliers of IT equipment are formally requested by the IT service and vetted by the Procurement service before being added as a recognised supplier within the purchasing system.

10.16 There is a limited number of IT staff who can raise Purchase Order requisitions. These requisitions then have to be electronically authorised through the purchasing system by the Head of Technology or the Head of Information Services and Business Support.

10.17 Items can only be procured using procurement cards or official Purchase Orders. Procurement cards are allocated to individuals who require them and only IT staff can use them to procure IT systems and services. Transactions made on procurement

cards for technology items are authorised by the Head of Technology or the Head of Information Services and Business Support.

10.18 Monthly meetings between Finance and the Head of Information Services and Business Support take place where budgets and spending figures are discussed and checked. The Head of Information Services and Business Support has intimated that the budgetary reporting from Finance could be improved by using "Business Objects" reporting software which would allow budget holders to electronically drill down into detailed records.

Recommendation: 4	Priority: 3
Consideration be given to the development of electronic reporting for budget holders to enable a more accurate approach to monthly reconciliation.	

10.19 It is understood that projects are not given their own budget codes to book equipment and services to. This makes project costing difficult to monitor and the Head of Information Services and Business Support has indicated that he has been specifically instructed to not keep his own records for purchasing.

Recommendation: 5	Priority: 3
Consideration be given to providing temporary budget codes for projects to enable accurate costing and reconciliation against agreed budgets.	

Risk Information assets being lost or stolen, which could breach confidentiality.

10.20 Hardware is marked with asset labels prior to deployment. The asset number is the serial number of the machine. Computer names reflect the asset number and are prefixed with various letters and numbers which represent the location of the device. By searching Active Directory and DHCP the physical location of any network connected machine can be found. It was demonstrated to Internal Audit that the location of a given machine could be identified.

10.21 Laptops are configured for the use by two persons maximum and would have to be reconfigured to use by other staff. Laptops are signed out on "Syops" forms and a record is maintained. It is noted that on previous audits that some equipment proved difficult to locate such as mobile phones (which are also on the Syops forms) and therefore it is suggested that a sample check of mobile equipment be undertaken periodically.

Recommendation: 6	Priority: 2
Regular sample checks be undertaken to ensure equipment registers are accurately maintained.	

10.22 It is understood that there is no co-ordinated incentive within FHQ to identify and return redundant equipment which could be recycled for use elsewhere rather than having to purchase new equipment.

Recommendation: 7	Priority: 3
An internal equipment usage audit be undertaken to identify under-utilised equipment for redistribution.	

10.23 User owned devices cannot be connected to the network without the permission and intervention of the IT service.

10.24 It is understood that printers and MFD's (Multi Function Devices, such as digital copiers) are purchased from the IT budget and therefore can be purchased by departments. These devices cannot be connected to the network or equipment without the permission and intervention of the IT service.

Risk Assets being disposed of inappropriately, potentially providing unauthorised access to data.

10.25 Hard drives are removed from redundant equipment and stored securely in a separate cage in the basement of FHQ. Once a number of drives have been collated a specialist company is used who securely shred the hard drives on the premises. A certificate of destruction is provided to the authority detailing the number of drives destroyed. This is matched to the number of drives provided for shredding. The machines (minus hard drives) are collected by another recycling company in line with the WEEE directive.

Risk Inappropriate use of email and Internet facilities bring the Force into disrepute.

10.26 In addition to the Force Information Security Policy there is an Email and Internet Acceptable Use Policy (AUP). This is available to all staff on the Intranet and details the requirements of staff when using these systems and the monitoring arrangements.

10.27 SPAM control for emails is managed by two separate systems. Incoming mail is first checked using a SPAM service on a watchguard firewall. This system is not very manageable and is therefore used as the first line of defence to remove items classed as genuine SPAM. The second system is ProofPoint which provides a more granular approach to quarantining suspected SPAM. These systems are checked several times a day by the Service Desk team and can release genuine emails to their recipients. If a user suspects an expected email has been quarantined by mistake, they can make a service request to the Service Desk team for investigation.

10.28 The ProofPoint system is also configured to hold emails, both incoming and outgoing, that meet certain predefined criteria, such as specific keywords, to ensure sensitive information can be checked by PSD before being released.

10.29 Several emails were checked by Internal Audit and it is noted that there are several different signature styles in use. Consideration should be given to defining and promoting a standard email signature to ensure outbound email communications have a professional look to them.

Recommendation: 8	Priority: 3
Consideration be given to formalising email signatures to ensure all outbound communications look professional.	

10.30 Web-filtering is undertaken using m86 (now Trustwave) products. Users are restricted from visiting undesirable websites defined by both category and individual URL blacklists.

Risk The Authority suffering legal action or adverse publicity due to the use of unlicensed software.

10.31 Microsoft licenses are purchased from a Microsoft partner (Phoenix). The licenses are held electronically. Specialist software is purchased from specific vendors and again it is understood that licenses are held electronically in a CMDB (Configuration Management Data Base). It is understood that Microsoft have recently audited the Authority's licenses and no significant issues were identified as a result.

10.32 Users do not have sufficient privileges to install software onto their machines. This must be performed by IT staff and is only undertaken if sufficient licenses are available and the license is owned by the Authority.

10.33 In response to the Microsoft License audit, the IT function is currently preparing a report of all software installations across the corporate network using Microsoft's SCCM (System Centre Configuration Manager) to extrapolate the information electronically for all software vendors from connected machines. Once the report is complete it will be compared to the licenses recorded in the CMDB to ensure compliance has been maintained.

Recommendation: 9	Priority: 2
Ensure that a full license reconciliation is undertaken once the SCCM report has been completed.	
