



Internal Audit Update Report for the Audit Committee December 2017

This document has been prepared for the Audit Committee to provide a status update in relation to the actions arising from Internal Audit Inspections.

Following the recent change of auditor the current Internal Audit Action Plan includes actions from both RSM and TIAA. The summary at the end of the action plan clearly states which auditor completed each report.

As follow up reports are no longer going to be produced by RSM their actions are being monitored by the Risk and Governance Board; with actions closed once the Force is satisfied processes have been implemented and form business as usual.

Since the last update (March 2017) twenty two actions have been closed (12 RSM and 10 TIAA); from either TIAA follow up reports or through internal reviews of the actions and updates, as stated above.

There remain 5 live actions from the RSM reports; of which 3 have implementation dates of March 2019 so are currently work in progress. All are being monitored, with regular updates provided by their owners.

There are thirteen live actions from the TIAA reports; only two have missed their implementation dates and the Force is working hard to rectify this and agree realistic timescales for implementation.

The action plan below provides details of the current actions with status updates, where applicable, from the action owners.

It should be noted that the RAG status reflects the nature of the recommendation rather than the completion status. The key to the colours can be found at the end of the report.

Gill Currie
HMIC Liaison Officer
Cleveland Police

Summary of All Outstanding Internal Audit Recommendations – Oldest Implementation Date First

No	Ref	Action Owner	Audit Finding	Implementation Date		Agreed Management Action	Status
				Original	Revised		
235	3.1 CGF16	Chief Finance Officer	The Joint Corporate Governance Framework did not reflect the responsibilities of the Head of HR or Head of Legal Services as benchmarked against other forces.	End July	August 2018	<p>The Force will consider the benefits of further articulating the delegated functions of other staff including the Head of Legal Services and Head of Human Resources in-line with sector best practice.</p> <p><u>October 2016 Update</u> This will be considered by the end of January 2017.</p> <p><u>March 2017 Update</u> This will be included in the review of governance arrangements to be undertaken as part of the changes to the Executive Team Structure and the establishment of the Corporate Services function.</p> <p><u>Update November 2017</u> To remain live as it will be reviewed in line with the annual update of the Joint Corporate Governance.</p> <p><u>Meeting 16th November JG and GC</u> Action to remain live until the update of the JCG report is produced.</p>	
250	EM16	Supt Mark Thornton	<p>A formal and robust policy will be put in place for the administration and maintenance of lockers so the process is consistent across all locations. Ahead of putting this policy in place there will be consideration of what lockers are used for so the policy has clarity of what can and can't be stored in them and what size lockers are required for each role. Staff will be informed when given a locker of items they can keep in them. The requirement for spot checks will be assessed and policy updated accordingly. If this assessment finds that lockers are currently being used as intended there may be no need to change current practice. If they are not then enforcement of locker spot checks should be considered.</p> <p>(Med)</p>	31st March 2019		<p><u>March 2017</u> This work is being undertaken as an integral part of the exit strategy from HQ which will take place by Autumn 2017. With staff transitioning into other operational units a full review of locker allocation, usage and maintenance is being undertaken. A forward strategy will be developed to maintain adequate system oversight for lockers. The senior responsible officer for this risk is now transferred to Superintendent Mark THORNTON.</p> <p><u>28th October 2017</u> Barry Plumpton has been tasked with carrying out an 'audit' during which he will be confirming names of staff with each locker, locating unused lockers, identifying staff who have numerous lockers in more than one site and making a record of locks which need to be replaced or new keys purchased, Barry is not responsible for any allocation.</p> <p>The management of lockers was previously a responsibility of Sopra Steria, however through Strategic Intent; staffing numbers and many of the tasks Sopra Steria previously performed were reduced. This was a Force decision, however Helen Turners team in Sopra Steria have offered to assist in part of the process whilst the audit takes place and a process for the future is agreed. In addition to this work the Estates Team have also assisted by completing a process of asset tagging all lockers in each location, this then ensures that there is the correct number of lockers in each location against the establishment.</p> <p>I (Mark Thornton) have discussed the issues with both Sopra Steria and Cleveland Police colleagues and I am mapping the full process which will be shared with all parties, I am seeking the co-operation of the IRT & INT Command Supervision, HR and Sopra Steria to bring this problem to a solution.</p> <p>Meeting invites will be sent to the parties already mentioned.</p> <p><u>Meeting 16th November JG and GC</u> Action remains on-going and is in line with the implementation date.</p>	
251	EM16	Supt Mark Thornton	<p>A reconciliation will be carried out (and then repeated periodically) at each site to identify all physical lockers, their size and their location to ensure this matches the details held on each locker spread sheet and there are no missing details on the spread sheets.</p> <p>The locker spread sheets will then be reconciled to the HR list of current staff, to ensure only current staff at each site are allocated a locker there and that the allocation of the locker is appropriate for their role.</p> <p>(High)</p>	31st March 2019		<p><u>March 2017</u> This work is being undertaken as an integral part of the exit strategy from HQ which will take place by Autumn 2017. With staff transitioning into other operational units a full review of locker allocation, usage and maintenance is being undertaken. A forward strategy will be developed to maintain adequate system oversight for lockers. The senior responsible officer for this risk is now transferred to Superintendent Mark THORNTON.</p> <p><u>28th October 2017</u> Barry Plumpton has been tasked with carrying out an 'audit' during which he will be confirming names of staff with each locker, locating unused lockers, identifying staff who have numerous lockers in more than one site and making a record of locks which need to be replaced or new keys purchased, Barry is not responsible for any allocation.</p> <p>The management of lockers was previously a responsibility of Sopra Steria, however through Strategic Intent; staffing numbers and many of the tasks Sopra Steria previously performed were reduced. This was a Force decision, however Helen Turners team in Sopra Steria have offered to assist in part of the</p>	

Summary of All Outstanding Internal Audit Recommendations – Oldest Implementation Date First

						<p>process whilst the audit takes place and a process for the future is agreed. In addition to this work the Estates Team have also assisted by completing a process of asset tagging all lockers in each location, this then ensures that there is the correct number of lockers in each location against the establishment.</p> <p>I (Mark Thornton) have discussed the issues with both Sopra Steria and Cleveland Police colleagues and I am mapping the full process which will be shared with all parties, I am seeking the co-operation of the IRT & INT Command Supervision, HR and Sopra Steria to bring this problem to a solution.</p> <p>Meeting invites will be sent to the parties already mentioned.</p> <p><u>Meeting 16th November JG and GC</u> Action remains on-going and is in line with the implementation date.</p>	
252	EM16	Supt Mark Thornton	<p>The process for new starters or transferred staff will be reviewed to ensure the team allocating lockers are informed of the additional locker requirements so they can ensure the correct locker is allocated. As part of the leaving process and transfer process, there will be communication with the staff managing the allocation of locker keys so they can request the return of locker keys. All keys will be returned to these locker staff so they can update the spread sheet with the next officer allocated to that locker. When officers are re-allocated, locker staff will confirm with staff at the officers' previous location to ensure they have returned their locker key and emptied their lockers before allocating them a locker at the new site. This process should be detailed in the policy proposed in management action one. The policy should also establish ownership and clear responsibilities of the management of lockers and management of the locker spread sheets. A lead contact will be established at each site for the staff managing lockers to escalate any issues to.</p> <p>(Med)</p>	31st March 2019		<p><u>March 2017</u> This work is being undertaken as an integral part of the exit strategy from HQ which will take place by Autumn 2017. With staff transitioning into other operational units a full review of locker allocation, usage and maintenance is being undertaken. A forward strategy will be developed to maintain adequate system oversight for lockers. The senior responsible officer for this risk is now transferred to Superintendent Mark THORNTON.</p> <p><u>28th October 2017</u> Barry Plumpton has been tasked with carrying out an 'audit' during which he will be confirming names of staff with each locker, locating unused lockers, identifying staff who have numerous lockers in more than one site and making a record of locks which need to be replaced or new keys purchased, Barry is not responsible for any allocation.</p> <p>The management of lockers was previously a responsibility of Sopra Steria, however through Strategic Intent; staffing numbers and many of the tasks Sopra Steria previously performed were reduced. This was a Force decision, however Helen Turners team in Sopra Steria have offered to assist in part of the process whilst the audit takes place and a process for the future is agreed. In addition to this work the Estates Team have also assisted by completing a process of asset tagging all lockers in each location, this then ensures that there is the correct number of lockers in each location against the establishment.</p> <p>I (Mark Thornton) have discussed the issues with both Sopra Steria and Cleveland Police colleagues and I am mapping the full process which will be shared with all parties, I am seeking the co-operation of the IRT & INT Command Supervision, HR and Sopra Steria to bring this problem to a solution.</p> <p>Meeting invites will be sent to the parties already mentioned.</p> <p><u>Meeting 16th November JG and GC</u> Action remains on-going and is in line with the implementation date.</p>	
270	FTSR16	Sergeant Kevin Taylor, Firearms Operations	<p>The Force will undertake a post implementation review to ascertain if the benefits of the Chronicle system have been realised.</p> <p>(Medium)</p>	31 January 2017	April 2018	<p>The Force currently does utilise the Chronicle system to manage its firearms. Discussions with the Sergeant - Firearms Operations noted that there had been no post implementation review of the Chronicle system to ensure that the project objectives had been achieved.</p> <p>Follow Up Report May 2017 – Action reiterated and now changed to High</p> <p><u>Update 13th October 2017</u> The technical infrastructure at the Tactical Training Centre has now been installed. JML (Chronicle) have been consulted with and will be undertaking a health check of our system and will assist in providing some advice in order for us to develop a plan to move forward which may include the requirement for further training that will incur some costs as yet unknown. It is hoped that the health check will take place before the end of the year.</p> <p><u>Meeting 16th November JG and GC</u> Action to remain live; awaiting outcome of health check. A new target date has been implemented.</p>	

Summary of All Outstanding Internal Audit Recommendations – Oldest Implementation Date First

278	ICS 2017	Ken Russell (Operational Security Manager)	<p>It was noted during the audit that there are known issues with particular security patches not being applied to systems due to third party dependencies. An example of this is the Smartworks system, where the supplier is currently unable or unwilling to endorse upgrading the version of the system and enable patching to the recommended standard.</p> <p>Recommendation ICT to perform an exercise of reviewing and documenting cases where there are patching concerns due to the third party supplier. Once this completed management to prioritise areas of concern according to risk and develop a plan to address the issues.</p>	31/10/17	31/3/18	<p><i>A specific information security schedule is to be implemented to ensure patching governance is part of future contractual requirements. In the meantime, we have identified the key suppliers that are not contractually bound to address patching concerns. A plan is now required to understand what supplier action can be taken and any compensating controls that can be implemented to address any gaps as much as possible.</i></p> <p>Update 27/10/17 16/10/2017 Ken Russell A specific information security schedule is to be implemented to ensure patching governance is part of future contractual requirements. In the meantime, we have identified the key suppliers that are not contractually bound to address patching concerns. A plan is now required to understand what supplier action can be taken and any compensating controls that can be implemented to address any gaps as much as possible,</p> <p>The security schedule is in progress and on track. Key suppliers are Capita. Capita stands alone in that addressing patches requires software upgrades so that Capita is able to support latest platform changes.</p> <p>Meeting 16th November JG and GC Action remains on-going with a new implementation date provided.</p>	
279	ICS 2017	Ken Russell (Operational Security Manager)	<p>Review of ITHC issues logs and reporting during testing identified that there are 3 'Critical' and 9 'High' rated issues identified as part of the last IT Health Check that had not been fully resolved at the time of the audit.</p> <p>Recommendation ICT management aim to resolve/mitigate remaining issues prior to PSN/ PSNP submission if possible. Where this is not practical management to document the specific tasks remaining, the planned start and finish dates of this work and the owner of the work as part of the Remediation Action Plan (RAP).</p>	30/9/17	December 2018	<p><i>The 3 critical issues have been remediated. 5 of the 9 high rated issues have been remediated. The remaining 4 have been discussed with the SIRO with interim acceptance given due to the complex nature and project planning required to remediate.</i></p> <p>Update 27/10/17 16/10/2017 Ken Russell The 3 critical issues have been remediated. 5 of the 9 high rated issues have been remediated. The remaining 4 have been discussed with the SIRO with interim acceptance given due to the complex nature and project planning required to remediate. Planning will be discussed and prioritised in accordance with the number of changes taking place in 2018.</p> <p>Update November 2017 The remaining 4 issues are broken down as follows: 1. Missing Apache Tomcat Patches <i>This is vendor dependant as the solution we use is only accredited to this version of Tomcat. There are no plans for updates at the moment and we are now awaiting quotes to understand the cost of forcing a vendor upgrade.</i> 2. Open SSH Missing Patches <i>This is dependent on 4 being completed.</i> 3. The TCP implementation in Cisco products allows remote attackers to cause a denial of service <i>This is dependent on 4 being completed.</i> 4. Cisco IOS 12.2, 12.4, 15.0, 15.2, and 15.3, when a VRF interface is configured, allows remote attackers to cause a denial of service <i>At the moment there are integration issues above version 12.2.2 with the Sophos Proxy Server which requires root cause analysis. However, a wider issue to address network-wide encryption to become industry compliant is being discussed which will absorb this issue as part of the project goals. Timescales for this are still to be agreed and could be as late as 2019 due to resources being invested in CSH project priorities. This project will impact all aspects of Cleveland Police and requires a considerable amount of planning, testing and assurance to ensure services are not impacted across network, network access and application use.</i></p> <p>These outstanding findings are now part of the Security Improvement Plan (SIP) and are being tracked monthly with Oliver Plumptre and Andy French and within the Information Security Board meetings with Simon Nickless. Whilst end dates are still tenuous, we are working to produce a plan so we can begin setting expectations.</p> <p>Currently mitigating controls are in place including:</p> <ul style="list-style-type: none"> Physical Security, 	

Summary of All Outstanding Internal Audit Recommendations – Oldest Implementation Date First

						<ul style="list-style-type: none"> • Role-based Access Controls, • limitations on force computer equipment making it only possible for threats to be internal and with privileged access, • Anti-Virus and Anti-Malware controls, • Protective Monitoring, monitoring failed access, privilege access, remote and network access <p>Meeting 16th November JG and GC Action to remain live until remaining issues are remedied.</p>	
280	ICS 2017	Ken Russell (Operational Security Manager)	<p>Microsoft withdrew support for their Windows Server 2003 and Windows XP operating systems in 2014 and 2015 respectively, from which time bug fixes and new vulnerabilities are no longer being addressed.</p> <p>Review of the Force's server infrastructure during the audit identified six servers using the out of date Windows 2003 operating system, and seven machines running Windows XP</p> <p>Recommendation ICT management to ensure that the out of support servers and machines are decommissioned and replaced and services migrated as soon as practical. Where this is not possible management should ensure risk acceptance has been documented.</p>	Q2 2018		<p>Cleveland have 6 XP desktop systems, 5 of which have a solution in progress. The remaining XP system requires the replacement of a specialist scanner which requires budget approval from the force. Each system is isolated from the network in terms of Internet and email access.</p> <p>Cleveland have 3 Windows 2003 servers, 2 are due to be decommissioned as part of two projects being progressed. The third Server to be decommissioned by the end of Q2 2018 due to business planning and budget constraints. A security plan is to be devised to ensure that this system is further locked down as much as possible to limit network exposure.</p> <p>ICT are meeting with the business in October to accelerate this process.</p> <p>Update 27/10/17 16/10/2017 Ken Russell Cleveland have 6 XP desktop systems, 5 of which have a solution in progress. The remaining XP system has been rendered standalone with network access permanently disabled. Each system is isolated from the network in terms of Internet and email access.</p> <p>Cleveland have 3 Windows 2003 servers, 2 are due to be decommissioned as part of two projects being progressed. The third Server to be decommissioned by the end of Q2 2018 due to business planning and budget constraints. A security plan is to be devised to ensure that this system is further locked down as much as possible to limit network exposure.</p> <p>Meeting 16th November JG and GC Action remains on-going and is within the implementation timeframe.</p>	
284	EMS2017	Richard Marron	<p>The following Policies and procedures should be brought up to date and each document to have version control:</p> <p>a) Standard Operating Procedures - This is a Steria document and by using flowcharts describes the various procedures for maintaining the estate. This was last updated in December 2011 and as such requires an update and refresh.</p> <p>b) Near Miss Procedure - A procedure for dealing with incidents and/or a dangerous occurrence. This was last updated/reviewed in March 2014 and may require a refresh.</p>	<p>a) 31st December 2017</p> <p>Completed 6th October 2017</p>	Discharged	<p>Recommendation The following procedures be updated: a) Standard Operating procedure and b) Near Miss Procedure and to have version control.</p> <p>Management Comments a) Standard Operating Procedure (SOP) document is to undergo a full review following changes to both the service delivered and contract with Cleveland Police, implemented over the past 12 months. This will include a version control heading b) Near miss procedure. SopraSteria have updated this document including version control</p> <p>Update November 2017 a) has a deadline of 31st December 2017 and SopraSteria estates team are working towards this b) has been completed and discharged</p> <p>Meeting 16th November JG and GC Part A remains on-going. An update has been requested from the action owner as he has resigned from the Force and is due to leave by the end of Q3 2017/18.</p>	
285	EMS2017	<p>a) Gill Currie</p> <p>b) Maria Hopper</p>	<p>A review of procedures that the Estates team refer to but are under the management of other teams within the Force noted that there were 10 which were either overdue a review or had not been subject to a review.</p>	<p>a) Policies: - 30th November 2017</p> <p>b) Records Management Plan and Management Retention Schedule: 31st May 2018.</p>		<p>Recommendation All policies and procedures that are not under the control of the Strategic Estates and Facilities Manager, (as in Paragraph 11.8) but are out of date, be reviewed and updated with version control at the earliest opportunity.</p> <p>Management Comment This work is already underway with all policies and procedures that require a review being completed by November 2017 and May 2018 check TH).</p> <p>Update November 2017 a). All policy and guidance documents have version control details at the end of the document. Policies /</p>	

Summary of All Outstanding Internal Audit Recommendations – Oldest Implementation Date First

						<p>Guidance are deemed valid until such a time as they are replaced or deleted. All outstanding policies are regularly chased and reported to the Risk and Governance Board, and subsequently the Management Board; a number remain outside of their review date.</p> <p>b).The RETENTION POLICY will be reviewed as part of the GDPR Readiness plan, this must be in place by 25/5/2018.</p> <p><u>Meeting 16th November JG and GC</u> Remains ongoing. All overdue policies chased with JG copied in. This will be taken to the next Management Board in December 2017.</p>	
286	HRAM17	Head of HR	With regard to Return to Work Interviews, it was noted that these had not always been carried out and recorded as having been completed on the system.	31/3/18		<p>Recommendation It be ensured that Return to Work Interviews are conducted in a timely manner for all police officers and staff returning from bouts of sickness and that these are appropriately recorded within Oracle.</p> <p>Management Comment: <i>Substantial work is being undertaken to rescope and redefine the way that HR service delivery meets the needs of the organisation. A business case is being developed which will be presented at December's Management Board to describe the growth and investment required to deliver enhanced levels of service to our people. If the business case is approved, the way that we manage all aspects of attendance will change radically, and responsibility for compliance will sit entirely with HR.</i></p> <p><u>Meeting 16th November JG and GC</u> Action remains on-going and is within the implementation timeframe.</p>	
287	HRAM17	Head of HR	For one police officer who was off sick until 3rd November 2017, it was found that their fit notes only covered until 31st October 2017. For two police officers, no fit notes could be located on the system.	31/3/18		<p>Recommendation It be ensured that doctors' Fit Notes are obtained for the entire period of sickness absence and appropriately stored on the system.</p> <p>Management Comments <i>Substantial work is being undertaken to rescope and redefine the way that HR service delivery meets the needs of the organisation. A business case is being developed which will be presented at December's Management Board to describe the growth and investment required to deliver enhanced levels of service to our people. If the business case is approved, the way that we manage all aspects of attendance will change radically, and responsibility for compliance will sit entirely with HR.</i></p> <p><u>Meeting 16th November JG and GC</u> Action remains on-going and is within the implementation timeframe.</p>	
288	HRAM17	Head of HR	With regard to attendance triggers, testing revealed that Attendance Management Meetings and Support Plans had not been put in place nor had the cases been referred to an Employee Relations Advisor.	31/3/18		<p>Recommendation Where attendance triggers are met, Attendance Management Meetings with police officers/police staff be held and appropriate Attendance Management Plans be put in place. In addition, these cases be referred to an Employee Relations Advisor who can assist with and provide guidance on sickness absence management processes.</p> <p>Management Comments <i>Substantial work is being undertaken to rescope and redefine the way that HR service delivery meets the needs of the organisation. A business case is being developed which will be presented at December's Management Board to describe the growth and investment required to deliver enhanced levels of service to our people. If the business case is approved, the way that we manage all aspects of attendance will change radically, and responsibility for compliance will sit entirely with HR.</i></p> <p><u>Meeting 16th November JG and GC</u> Action remains on-going and is within the implementation timeframe.</p>	
289	HRAM17	Head of HR	Not all cases who had met the 28 days absence trigger had been referred to the Force Medical Advisor. In addition for two police officers who had since returned to work following long bouts of	31/3/18		<p>Recommendation All cases of sickness absence in excess of 28 days are referred to the Force Medical Advisor in a timely manner in accordance with procedures.</p> <p>Management Comments <i>Substantial work is being undertaken to rescope and redefine the way that HR service delivery meets the</i></p>	

Summary of All Outstanding Internal Audit Recommendations – Oldest Implementation Date First

			sickness it was found that they had not been referred to the Force Medical Advisor until sometime after they had returned. It was not possible to determine why they had not been referred whilst they were off sick.			<p><i>needs of the organisation. A business case is being developed which will be presented at December's Management Board to describe the growth and investment required to deliver enhanced levels of service to our people. If the business case is approved, the way that we manage all aspects of attendance will change radically, and responsibility for compliance will sit entirely with HR.</i></p> <p>Meeting 16th November JG and GC Action remains on-going and is within the implementation timeframe.</p>	
290	HRAM17	Strategic HR Advisors	For one staff member it was noted that their Return to Work Interview was recorded as having taken place on 22nd November 2016. However, this date is also recorded as the staff member's last day of absence which means either the date they returned to work or the date recorded for the Return Work Interview has been incorrectly input.	30/11/17		<p>Recommendation Line managers to be reminded of the importance of inputting the correct date for each stage of the sickness absence management process.</p> <p>Management Comments <i>Ongoing. Managers guidance is sent with the weekly sick report, and also reported into TPG</i></p> <p>Meeting 16th November JG and GC Action remains on-going and is within the implementation timeframe.</p>	
291	KFC2017	Ged Gallagher	It was advised that the Oracle system does not permit a report to be run to identify when supplier banks details have been changed. Testing identified that the checking of supplier details changes is not undertaken as a standard control, although there was evidence to support that it had been undertaken for four out of five bank account changes that were able to be identified from hardcopy paperwork held by the Finance team.	31/12/17		<p>Recommendation All supplier account detail changes be verified with the supplier using existing contact details before the change is made.</p> <p>Management Comments <i>Note: there is an audit log which identified who made the last change to an account. However we have since written a bespoke report which provides greater clarity regarding the changes.</i></p> <p>Meeting 16th November JG and GC Action is complete and will be reviewed by TIAA on their review of recommendations audit</p>	
292	KFC2017	Ged Gallagher	It was advised that the Oracle system does not permit a report to be run to identify when supplier banks details have been changed. The use of having such a report would allow a check of any changes that may have been made between each payment run.	31/12/17		<p>Recommendation Investigations be undertaken to identify if the Oracle system can be utilised to provide a report that identifies supplier detail changes, which would allow a check to be undertaken prior to each payment run.</p> <p>Management Comments <i>Note: there is an audit log which identified who made the last change to an account. However we have since written a bespoke report which provides greater clarity regarding the changes.</i></p> <p>Meeting 16th November JG and GC Action is complete and will be reviewed by TIAA on their review of recommendations audit</p>	
293	KFC2017	Ian Hailstone	A review of the user accounts on Oracle for Accounts Payable and Accounts Receivable noted that there were four users plus an Administrator who had Receivables Super User Status, however, it was identified that three of these also had a separate account designated as Receivables User, which appeared to be a duplicate.	30/11/17		<p>Recommendation A review of the duplicated accounts with Receivables Super User and Receivable User permissions be undertaken to determine if both accounts are required.</p> <p>Management Comments <i>Note: These were not duplicate accounts. The user only had one account to access the system, however the account had two levels of responsibility within the account. We have removed the lower level as it was established the functionality within the "Super User" was the required level for the role.</i></p> <p>Meeting 16th November JG and GC Action is complete and will be reviewed by TIAA on their review of recommendations audit</p>	
294	SCCG 2017	CFO - CC	While the Joint Corporate Governance Framework is a comprehensive document it does require at least an annual review to confirm all sections are relevant and have current data within. There are several sections of the	June 2018		<p>Recommendation The Joint Corporate Governance Framework be reviewed annually and be reported to the Management Board and Audit Committee accordingly.</p> <p>Management Comment <i>The Joint Corporate Governance Framework will be reviewed annually and will be reported to the Management Board and Audit Committee on an annual basis.</i></p>	

Summary of All Outstanding Internal Audit Recommendations – Oldest Implementation Date First

			Joint Corporate Governance Framework that are out of date and need updating/reviewing. This should be done at an early time and reported to the Management Board and then to the Audit Committee. In addition, version control needs to be incorporated within the document.				
--	--	--	--	--	--	--	--

Reference key to Audit Reports:

Reference	Report Title	Published	Presented to Audit Committee
CGF16	Corporate Governance Framework 2016 RSM	May 2016	23/6/16
EM16	Estate Management – Lockers 2016 RSM	November 2016	16/12/16
EMS2017	Estates Management Strategy 2017 TIAA	October 2017	14/12/17
FTSR16	Firearms Taser Service Records 2016 RSM	September 2016	22/9/16
HRAM17	HR Attendance Management 2017 TIAA	November 2017	14/12/17
ICS2017	ICT Cyber Security 2017 TIAA	September 2017	14/12/17
KFC2017	Key Financial Controls 2017 TIAA	November 2017	14/12/17
SCCG2017	Strategic Control and Corporate Governance 2017 TIAA	November 2017	14/12/17

	High / Priority 1 / Urgent
	Medium / Priority 2 / Important
	Low / Priority 3 / Routine