

|  |
| --- |
| **The Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police** |
| **Assurance Review of ICT Cyber Security**  **2017/18** |

|  |
| --- |
| **Executive Summary** |

|  |  |
| --- | --- |
| **OVERALL ASSURANCE ASSESSMENT** | **KEY FINDINGS** |
|  | **The key outcomes form this audit include:**   * **There were delays in applying critical security patches to key servers;** * **The inability to patch certain systems/ servers due to third party dependencies;** * **There were three ‘Critical’ and nine ‘High’ rated issues identified as part of the last IT Health Check reporting which remain open;** * **There were seven PCs and six servers that were found to be running out-of-support operating systems;** * **There are deficiencies in the current Protective Monitoring process.** |
| **SCOPE** | **ACTION POINTS** |
| The objective of the audit was to provide an opinion on whether adequate Cyber Security process and controls have been implemented to provide adequate protection to the Cleveland Police network domain.  The audit consisted of a high level review of key controls required for CES accreditation including the following;   * Firewall security and intrusion prevention; * Internal vulnerability scanning and external penetration testing; * Management of Active Directory and Network privileged access rights; * Malware protection policies and deployment of anti-malware software; * Patch Management policies and procedures. | |  |  |  |  | | --- | --- | --- | --- | | **Urgent** | **Important** | **Routine** | **Operational** | | **0** | **4** | **3** | **5** | |

|  |
| --- |
| **Management Action Plan – Priority 1, 2 and 3 Recommendations** |

| **Rec.** | **Risk Area** | **Finding** | **Recommendation** | **Priority** | **Management**  **Comments** | **Implementation**  **Timetable**  **(dd/mm/yy)** | **Responsible**  **Officer**  **(Job Title)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | Compliance | During review of patching processes it was noted that there is currently an issue with critical system server patching not being applied to servers supporting key systems on a timely basis.  There has historically been difficulty in scheduling downtime during which to apply patches on servers supporting systems such as Pro Centre, STORM, Niche and Oracle ER because of the perceived impact to services. | Operational Security Manager to identify a regular monthly patching window and agree this with the business. | 2 | *Server patch process has been agreed and will conform to GDS/PSN security patching requirements. Implementation will commence from October.*  *Critical security patches will be applied within 14 Days, Important security Patches will be applied within 30 days.* | *30/09/17* | *Ken Russell (Operational Security Manager)* |
| 5 | Compliance | 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. | 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. | 2 | *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.* | *31/10/17* | *Ken Russell (Operational Security Manager)* |
| 6 | Compliance | 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. | 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). | 2 | *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.* | *30/09/17* | *Ken Russell (Operational Security Manager)* |
| 7 | Compliance | 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.  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 | 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. | 2 | *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.*  *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.*  *ICT are meeting with the business in October to accelerate this process.* | *Q2 2018* | *Ken Russell (Operational Security Manager)* |
| 1 | Compliance | It was noted during the audit that although review of firewall settings may be performed on ad-hoc basis, there is no regularly scheduled and documented review process currently in place.  A regular, documented process would help in ensuring firewall rules remain appropriately restricted and that that rules that are no longer required are removed or disabled in a timely manner. | Operational Security Manager to conduct quarterly reviews of firewall security and update the Information Security Manager | 3 | *A quarterly review is now in place to review all border firewall appliance rule-sets. Results of each review are formerly documented with any findings triaged and actioned through Change Control processes.* | *30/09/17* | *Ken Russell (Operational Security Manager)* |
| 2 | Compliance | The Cyber Essentials Scheme Guidelines (CESG)’s ‘Protective Monitoring for HMG ICT Systems (GPG 13)’ guidance outlines recommendations and requirements around the protective monitoring of ICT systems for government and public sector organisations.  We found that the Log Rhythm tool is used to capture and generate logging and reporting in compliance with the GPG 13 guidance. It was noted however that that though events are logged and reporting is available there is not as yet a system in place to regularly review and act upon exceptions/ potential issues identified. | Operational Security Manager to develop a process around the receipt and review of Log Rhythm reports and an escalation process for passing out reporting and exceptions to the business/ system owners for actioning. | 3 | *The operational Security Manager now received the LogRhythm reports. A process is now in place to interpret the volume of detail to a summary dashboard to draw attention to potential issues. These are then escalated to ICT for triage and action if necessary. False positives will be learned and removed as part of this process.* | *30/09/17* | *Ken Russell (Operational Security Manager)* |
| 3 | Compliance | HM Government’s ‘Cyber Essentials’ scheme details a number of key requirements to be used for mitigating the most common Internet based cyber security threats.  This guidance details a number of requirements for ensuring the security and of user and administrator passwords.  It was noted that the password requirements in place for Administrator level accounts do not currently meet requirements around password length or the length of time required before a password change is enforced. | ICT management to investigate options around mitigating the risks around recommended password settings as part of the ongoing cyber essentials work. | 3 | *A review has been completed which determined only a very small number of administrative accounts failed policy compliance. Actions have now completed to ensure all administrator accounts now conform to the Cleveland Police password policy.* | *30/09/17* | *Ken Russell (Operational Security Manager)* |

|  |
| --- |
| **Operational Effectiveness Action Plan** |

| **Ref** | **Risk Area** | **Item** | **Management**  **Comments** |
| --- | --- | --- | --- |
| 1 | Compliance | There is not currently an active network intrusion detection system in use to identify potentially malicious activity. A cost/ benefit exercise around the implementation of an intrusion detection solution should be undertaken. | *The Cleveland Police network is isolated from the Internet. Network intrusion would require an internal threat with physical access to the Cleveland Police Network. Protective Monitoring is now working from an Operational Security Management perspective and we will continue to evaluate the needs of IDS/IPS based on these and other security metrics being monitored on a monthly or incident-based basis.* |
| 2 | Compliance | Although Nessus is used occasionally on ad-hoc basis to conduct internal vulnerability scanning, this is not performed on a regular basis. It is suggested as a process improvement that the Operational Security Manager consider implementing a regular internal vulnerability scanning process. | *The operational security manager will operate quarterly scans. This is to begin within Q4 2017, using Nessus.* |
| 3 | Compliance | There is a potential vulnerability in the email quarantine process as suspected spam email are not scanned by an AV solution and may be released by users via an emailed link. This means there is a potential route for malware to exploit in the event of users downloading an infected file. Management should review potential mitigations for this risk such as the implementation of a software solution or improved guidance to staff around the risk. | *Although Cleveland Police have adopted a process of self-release for emails that could be spam or legitimate. More has been done to strengthen user awareness for this process, with the email Quarantine regularly reviewed for potential spam/malicious email campaigns etc.*  *The ICT team are looking into new technologies such as Bromium to address this concern. A proof of concept will complete by the end of November 2017 to determine technology choice and business case for business approval and budget authorisation.* |
| 4 | Compliance | Microsoft’s System Center Configuration Manager 2012 (SCCM) is used to manage and deploy security patches with the exception of non-standard/ 3rd party applications which currently be patched manually. If is suggested that ICT management perform an exercise to quantify the benefits around procuring and utilising the Corporate Software Inspector (CSI) plugin that would enable SCCM to be used for this purpose. | *The budget for CSI has been authorised for procurement. It is envisaged that this will be deployed by the end of October and will conform to the Cleveland Police security patch policy & processes.* |
| 5 | Operational | Software assets are currently managed via the use of a manually maintained spreadsheet. It is suggested that management investigate options around the implementation of a software asset management system such as Snow. | *The CSH Cloud project is in the process of identifying Cleveland Police ICT assets. The project is due to complete by October 2018 where the asset register will be handed over to ICT and continued to be managed.* |

|  |
| --- |
| **Detailed Findings** |

**INTRODUCTION**

1. This review was carried out in July 2017 as part of the planned internal audit work for 2017/18. Based on the work carried out an overall assessment of the overall adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

**KEY FINDINGS & ACTION POINTS**

1. 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 for their full impact before they are implemented.

**SCOPE AND LIMITATIONS OF THE REVIEW**

1. The objective of the audit was to provide an opinion on whether adequate Cyber Security process and controls have been implemented to provide reasonable protection to the Cleveland Police network domain. The audit consisted of a high level review of key controls required for CES accreditation;

* Firewall security and intrusion prevention;
* Internal vulnerability scanning and external penetration testing;
* Management of Active Directory and Network privileged access rights;
* Malware protection policies and deployment of anti-malware software;
* Patch Management policies and procedures.

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan.

**MATERIALITY**

1. Cyber security processes and controls are intended to provide a minimum baseline of security in protecting the business against cyber threats such as malware or an external attack compromising the Force’s data, systems or services.

**DISCLAIMER**

1. 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. TIAA neither owes nor accepts 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.

**RISK AREA ASSURANCE ASSESSMENTS**

1. The definitions of the assurance assessments are:

|  |  |
| --- | --- |
| **Substantial Assurance** | There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved. |
| **Reasonable Assurance** | The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved. |
| **Limited Assurance** | The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved. |
| **No Assurance** | There is a fundamental breakdown or absence of core internal controls requiring immediate action. |

**ACKNOWLEDGEMENT**

1. We would like to thank staff for their co-operation and assistance during the course of our work.

**RELEASE OF REPORT**

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

|  |  |
| --- | --- |
| **Date draft report issued:** | 20th September 2017 |
| **Date management responses received:** | 26th September 2017 |
| **Date final report issued:** | 27th September 2017 |

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

|  |
| --- |
| **Directed Risk: Failure to direct the process through approved policy & procedures.** |

* 1. Key ICT policies and procedures relevant to cyber security were identified and obtained during the course of the audit. These were used in the process of reviewing the suitability of the controls in place around cyber security. The policies identified as being of particular relevance in this review are the; ‘Force Information Security Policy’, ‘Network Security Policy’, ‘Malware Security Policy’, and the ‘Security Patch Policy’.
  2. The policies are currently undergoing a process of review and being updated, however the overarching Information Security Policy reviewed on site was found to contain the expected level of detail and to have covered expected considerations including definition of key roles and responsibilities, references to relevant legislation and Freedom of Information Act issues.
  3. Policies and procedures are made available to staff via the intranet policy section. All staff are required to undertaken mandatory e-learning in a range of subjects, including information security and cyber security requirements. Data Protection and Freedom of Information requirements are also available via the NCALT e-learning system. It was also noted that there had been a recent Cyber Security awareness exercise involving providing guidance and information to staff over the course of a week.
  4. It was also identified that standard operating procedures, board reporting and also a risk management process was also in place.

|  |
| --- |
| **Compliance Risk: Failure to comply with approved policy and procedure leads to potential losses.** |

* 1. High level network diagrams describing the Cleveland Police network were obtained and reviewed in conjunction with ICT management during the audit. The network makes use of firewalls to ensure unauthorised traffic is not permitted. Firewall rules are annotated and configured based on the principle of ‘least privilege’, meaning that only the IP addresses and ports necessary for stated business functions are enabled.
  2. Administrator level access is required to make changes to firewall rules and this is limited to two authorised members of staff. All significant changes to the firewalls are made as part of the documented change process, with the exception of routine changes such as adding/ modifying IP addresses.
  3. Firewalls are subject to annual independent penetration testing in line with the IT Health Check and PSN/ PSNP accreditation processes. It was noted however that although internal review of firewall settings may be performed on ad-hoc basis, there is no regularly scheduled and documented review currently in place. A regular review process would help in ensuring firewall rules remain appropriately restricted and that rules that are no longer required are removed or disabled in a timely manner.

|  |  |
| --- | --- |
| **Recommendation: 1** | **Priority: 3** |
| **Operational Security Manager to conduct quarterly reviews of firewall security and update the Information Security Manager with any issues identified.** | |

* 1. An annual programme of IT Health Checks is undertaken as part of the ongoing PSN & PSNP compliance and accreditation processes. This exercise includes penetration testing of the network and firewalls, vulnerability testing of network infrastructure, anti-malware, and equipment that interacts with the network.
  2. During review of network design and security controls it was noted that there is not currently an active network intrusion detection system in use to identify potentially malicious activity. It is recommended that a cost/ benefit exercise around the implementation of an intrusion detection solution is undertaken.

|  |
| --- |
| **Operational Effectiveness Matter: 1** |
| **Operational Security Manager to undertake a cost/ benefit exercise around the implementation of an intrusion detection solution.** |

* 1. Although the Nessus vulnerability tool is used on an ad-hoc basis to conduct internal vulnerability scanning, this is not performed on a regular basis. Though this is not seen as mandatory due to the annual health check reporting, it is suggested as a process improvement that the Operational Security Manager considers implementing a regular internal vulnerability scanning process, as this will enable earlier detection of issues and improved assurance that vulnerabilities are being identified and resolved.

|  |
| --- |
| **Operational Effectiveness Matter: 2** |
| **Operational Security Manager to consider implementing a regular internal vulnerability scanning process.** |

* 1. The Cyber Essentials Security Guidelines (CESG)’s ‘Protective Monitoring for HMG ICT Systems (GPG 13)’ guidance outlines recommendations and requirements for the protective monitoring of ICT systems for government and public sector organisations. This includes requirements for collecting and reviewing ICT log information and configuring ICT logs in order to provide an audit trail of security relevant events of interest.
  2. The Log Rhythm tool is used to capture and generate logging and reporting in compliance with the GPG 13 guidance. It was noted however that that though events are logged and reporting is available there is not as yet a system in place to regularly review and act upon exceptions/ potential issues identified.

|  |  |
| --- | --- |
| **Recommendation: 2** | **Priority: 3** |
| **Operational Security Manager to develop a process around the receipt and review of Log Rhythm reports and an escalation process for passing out reporting and exceptions to the business/ system owners for actioning**. | |

* 1. HM Government’s ‘Cyber Essentials’ scheme details a number of key requirements to be used for mitigating the most common Internet based cyber security threats. This guidance details a number of requirements for ensuring the security of user and administrator passwords. User and Administrator network level password parameters were obtained and reviewed during the audit.
  2. It was noted that the password requirements in place for Administrator level accounts do not currently meet requirements around password length or the length of time required before a password change is enforced.
  3. It is understood from discussion with management that modifying password settings to comply with recommendations may be difficult and costly due to technical compatibility issues between Active Directory and Oracle systems, and that management will need to review options to determine whether there is a more practical solution.

|  |  |
| --- | --- |
| **Recommendation: 3** | **Priority: 3** |
| **ICT management to investigate options around mitigating the risks around recommended password settings as part of the ongoing cyber essentials work.** | |

* 1. In mitigation it was noted that the number of Domain Administrator accounts is strictly limited to 7 authorised members of staff, with a segregation of duties policy in place requiring that administration activities are performed on separate administrator accounts, rather than via the user’s normal AD network account.
  2. All servers and PCs/laptops are protected by a range of malware detection applications, with Sophos being used as the main AV solution. Removable media is subject to content analysis and anti-virus scanning, and devices are automatically denied to users until a request to use such devices is granted by the Information Security Manager.
  3. The Sophos email appliance is configured to review all email content and rules are in place to block suspect emails and quarantine them. Spam filtering is in place to automatically filter and delete any confirmed spam automatically and quarantine suspected spam for later release if necessary. It was noted however that there is a potential vulnerability in the email quarantine process. Under the existing process users are emailed a link in order to release the suspected spam email which is not scanned by an AV solution. This means there is a potential route for malware to exploit in the event of users downloading an infected file.

|  |
| --- |
| **Operational Effectiveness Matter: 3** |
| **Management to review potential mitigations for the risk around quarantined emails such as the implementation of a software solution or improved guidance to staff around the risk.** |

* 1. A documented patching process is in place to ensure systems are patched on a timely basis. This includes the required stages of risk assessment, approval, testing and deployment. Change control procedures for patching, including the documentation of contingency and back-out plans, were also found to be in place.
  2. Microsoft’s System Centre Configuration Manager 2012 (SCCM) is used to manage and deploy both desktop and server patches. It was noted that it was not currently capable of being used to patch non-standard/ 3rd party applications, and that these must currently be patched manually. It was noted that a third party plug in – Corporate Software Inspector (CSI) - was available that would enable SCCM to be used for this purpose. It is suggested that this would deliver the benefit of consolidating and standardising patching processes, reducing manual patching and the overall risk around systems not being patched on a timely basis.

|  |
| --- |
| **Operational Effectiveness Matter: 4** |
| **ICT management should perform an exercise to quantify the benefits around procuring and utilising the CSI plugin.** |

* 1. It was noted during review of patching processes that there is currently an issue with critical system server patching not being applied to key servers on a timely basis. There has historically been difficulty in scheduling downtime in which to apply patches on servers supporting key systems such as Pro Centre, STORM, Niche and Oracle ER because of the perceived impact to services.

|  |  |
| --- | --- |
| **Recommendation: 4** | **Priority: 2** |
| **Operational Security Manager to identify a regular monthly patching window and agree this with the business.** | |

* 1. It was also noted during discussion with ICT management that there are several known issues with particular system security patches not being applied due to third party dependencies. An example of this is the Smartworks system, where the supplier is currently unable or unwilling to support or endorse upgrading the version of the system to enable patching to the recommended standard.

|  |  |
| --- | --- |
| **Recommendation: 5** | **Priority: 2** |
| **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.** | |

* 1. PSN compliance requirements state that ‘Critical’ and ‘High’ issues identified as part of the annual IT Health Check that are not addressed by the time of submission must be reported as part of the submission along with detailed plans for how the issues will be addressed. PSNP requirements also require reporting of ‘Medium’ rated issues.
  2. It was noted that management has implemented a tracking and reporting system in order to better monitor and manage actions and associated issues arising from the annual IT Health Check report. Review of this reporting demonstrated that significant progress has been made in resolving/ mitigating issues identified in the most recent report with only 22 of the 208 reported issues remaining open at the time of the audit.
  3. Of the remaining 22 issues, there are 3 ‘Critical’ and 9 ‘High’ rated issues that have not been fully resolved as yet.

|  |  |
| --- | --- |
| **Recommendation: 6** | **Priority: 2** |
| **ICT management aim to resolve/ mitigate remaining issues prior to PSN 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).** | |

* 1. 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. 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.
  2. Although servers running the out of date operating systems will continue in most cases continue to work using the unsupported software, this increases the risks of viruses and other security threats impacting systems and services. We were advised that management is aware of the machines and servers in question and arrangements are were being put in place to decommission them as soon as possible.

|  |  |
| --- | --- |
| **Recommendation: 7** | **Priority: 2** |
| **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.** | |

|  |
| --- |
| **Operational Risk: Failure to identify opportunities to operate more efficiently or to be prepared for forthcoming changes.** |

* 1. Software assets are currently managed via the use of a manually maintained spreadsheet. It is suggested that management investigate options around the implementation of a software asset management system such as Snow.

This would assist by automating the process of software compliance and deliver potential benefits such as greater assurance that all software on the network has been identified, is licensed, and provides potential for efficiencies through the reporting of over licensing, under licensing and unused applications.

|  |
| --- |
| **Operational Effectiveness Matter: 5** |
| **ICT management to investigate options around the implementation of a software asset management system.** |

---------------