

Report to	<b>Audit Committee</b>
Date	<b>04/06/18</b>
Lead Officer	<b>Head of Audit and Procurement Services</b>
Contact Officer	<b>Keith Williams (Audit Manager)- 01492 576217</b>
Subject	<b>Internal Audit Annual Report 2017/18</b>



## **PURPOSE OF REPORT**

- 1 Under the terms of the Accounts and Audit regulations, the Authority is required annually to conduct a review of the effectiveness of its system of Internal Control. Internal Audit is an integral part of that system, and is a significant contributor to the preparation of the Annual Governance Statement, which is required to be included in the Annual Statement of Accounts.
- 2 The UK Public Sector Internal Audit Standards 2013 require the Head of Internal Audit to provide the Audit Committee with assurance on the whole system of internal control, including the adequacy of risk management and corporate governance arrangements.
- 3 The report contains the assurance statement based on the work of Internal Audit during the year ended March 2018.

## **EXECUTIVE SUMMARY**

- 4 The Head of Internal Audit is able to provide assurance to the Audit Committee, based on the internal audit work undertaken, together with our maintained knowledge of the organisation and its procedures, that the Authority has effective corporate governance, risk management and internal control arrangements to manage the achievement of the Authority's objectives.
- 5 The report identifies that 50 days of Internal Audit work was performed during 2017/18 as compared to a planned allocation of 55 days; as a result 5 days audit work will be carried forward into 2018/19.
- 6 The audit reviews provide a level of assurance upon the adequacy of the systems of internal control in place, although 39 recommendations have been made in the year to address some weaknesses. A formal follow up process is in place to ensure that the recommendations are implemented within agreed timescales.

- 7 The work of Internal Audit has not identified any weaknesses that would qualify this opinion and there are no significant issues that are relevant to the preparation of the Annual Governance Statement.
- 8 The report also provides assurance that the Internal Audit Service operates in compliance with the UK Public Sector Internal Audit Standards to enable the Authority to take assurance from this opinion.

## **RECOMMENDATIONS**

- 9 It is recommended that Members are asked to consider and provide comment on the assurance to the Audit Committee that for the 12 months to 31<sup>st</sup> March 2018, the Authority has satisfactory internal control, risk management and corporate governance process in place to manage the achievement of its objectives.

## **BACKGROUND**

### **The Role of Internal Audit**

- 10 Under the terms of The Accounts and Audit (Wales) Regulations 2014, Fire Authorities have a statutory responsibility to maintain “an adequate and effective system of internal audit.”
- 11 The role of Internal Audit Services is to provide management with an objective assessment of whether systems and controls are working properly. It is a key part of the organisation’s internal control system because it measures and evaluates the adequacy and effectiveness of other controls so that:
  - the Audit Committee and senior management are aware of the extent to which they can rely on the whole system; and
  - individual managers are aware of how reliable are the systems and controls for which they are responsible.
- 12 The internal control system comprises the whole network of systems and controls established to manage the Authority, to ensure that its objectives are met. It includes financial and other controls and also arrangements for ensuring that the Authority is achieving value for money from its activities.
- 13 The North Wales Fire and Rescue Authority (NWFRA) Financial Regulations state that a report shall be submitted under the auspices of the NWFRA as regards the performance against the original plan for the previous financial year.

## INFORMATION

### Review of 2017/18 Activity and Performance

- 14 A schedule giving an audit opinion of the adequacy and effectiveness of internal control processes and a summary of the key messages in respect of all the audit assignments undertaken during 2017/18 is attached at **Appendix A**.
- 15 Four audits reports were completed during the year covering:
- **Cyber Security (Part 1)** – The objective of the review was to provide management with an independent assessment relating to the effectiveness of cybercrime prevention, detection and incident management policies, procedures and governance activities. The review is in two parts, with this report covering Governance, Inventory of Assets and Standard Security Configurations. The audit findings demonstrated that key controls are in place but there are gaps, which leave NWFRS exposed to what could be significant risks, which results in a **Limited** assurance rating.
  - **Retained Stations (Conwy and Denbighshire)** – A review was undertaken to ensure retained firefighters are paid accurately and effectively, stations are effectively safeguarding their assets, vehicle usage is properly controlled and station welfare funds are operating in accordance with the SAPPO. The audit made 9 recommendations and provided a Satisfactory level of assurance.
  - **Whistleblowing Policy and Procedures** – A review of the Authority's whistleblowing policy and procedures was undertaken to provide a level of assurance to management that internal controls are operating effectively, potential risks are well managed and corporate objectives are being achieved. The audit made 12 recommendations and provided a Satisfactory level of assurance.
  - **National Fraud Initiative (NFI)** – NFI is a comprehensive and thorough 'data matching' exercise organised by the Cabinet Office in partnership with the Wales Audit Office (WAO). There were no issues arising from the investigations, which provides a High level of assurance that the systems of internal control are working well and that frauds and irregularities are being minimized. The exercise also assists to strengthen anti-fraud and corruption arrangements and instil an anti-fraud culture.
- 16 In addition, some work was undertaken by Internal Audit to support the Service's Senior Professional Services Manager in an internal investigation. The investigation related to information received by the Wales Audit Office (WAO) about the potential use of Service vehicles by

officers employed by NWFRS, which may be classified by the HMRC as a 'benefit in kind'. A report was completed by the Service, which made 4 recommendations to further strengthen the controls that were already in place; further work was performed by WAO in January 2018.

- 17 The outcome of each audit and the evaluation of the adequacy of the internal control environment is based on the number of recommendations and their risk rating. All audits undertaken during the year were assessed as providing positive levels of assurance, with the exception of the audit of Cyber Security, which made 18 recommendations and provided a Limited level of assurance. The audit is scheduled to be followed up early in 2018/19.
- 18 To address the weaknesses identified during the audit reviews 39 recommendations have been made. Action plans setting out the agreed response to the audit recommendations were issued with the audit reports and these have been returned from Fire and Rescue Authority management, completed with the action to be taken to ensure implementation of the recommendations. Management have agreed to implement all the audit recommendations.
- 19 To comply with CIPFA's Public Sector Internal Audit Standards 2013 a formal follow up process is in operation within the Section to confirm that the recommendations made in Internal Audit reports have been implemented by management within agreed timescales. A follow up audit will normally take place six months after the issue of the final report. A schedule of the follow up audits conducted during the period 1 April 2017 to 31 March 2018 is attached at **Appendix B**. It demonstrates the number of recommendations accepted and subsequently implemented by management in each area and reveals changes that impact on the original audit opinion. Further follow up work will be performed in those areas where a significant number of recommendations remain outstanding.
- 20 During 2017/18, 50 audit days were provided, as compared to a planned allocation of 55 days as indicated in the annual audit plan. A summary of audit activity is attached at **Appendix C** and shows the planned allocation of audit resources in terms of man days over departments and services and compares actual work done for 2017/18 with the plan.
- 21 The Cyber Security (Part 1) audit was not completed until December 2017 due to unforeseen circumstances; 7 days were allocated in the year to complete the audit and prepare the audit programme for Part 2 of the audit, which has been carried forward into 2018/19. This, together with additional work upon the Authority's Whistleblowing policies and procedures resulted in the planned Creditors (P2P System) audit being carried forward into 2018/19.

## **Internal Audit Plan 2018/19**

- 22 The Draft Annual Plan for 2018/19 is attached at **Appendix D**; the available audit resource has been increased to 55 days as a result of 5 days being carried forward from 2017/18. The purpose of the annual audit plan is to:-
- establish audit priorities in conjunction with Fire and Rescue Authority Management based upon a risk based approach of determining the audit needs of the Authority at the start of each year
  - determine the resources needed to carry out the required audit duties
  - review and follow up the audit work of the previous year.
- 23 The audit plan is designed to act as a guide only. Changes in circumstances or other unforeseen events may result in deviations from the plan. The plan for 2018/19 has been prepared following consultation with Fire and Rescue Authority Management. The plan also includes time to follow up recommendations from previous audits.

## **THE STATEMENT OF ASSURANCE**

### **Preamble**

- 24 The Head of Internal Audit is required to provide the Audit Committee with assurance on the whole system of internal control, including the adequacy of risk management and corporate governance arrangements. It should be noted that assurance can never be absolute. The most that Internal Audit can provide to the Audit Committee is a reasonable assurance that there are no major weaknesses in the whole system of internal control.
- 25 The matters raised in this report are only those that came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

### **Overall Assurance**

- 26 The work of Internal Audit Services has been conducted in compliance with CIPFA's Public Sector Internal Audit Standards 2013.

## **Audit Opinion**

- 27 I am satisfied that internal audit work undertaken, together with our maintained knowledge of the organisation and its procedures allow me to draw a reasonable conclusion as to the adequacy and effectiveness of the NWFRA risk management, control and governance processes. In my opinion, for the 12 months ended 31st March 2018, NWFRA has satisfactory internal control and corporate governance processes to manage the achievement of the Authority's objectives.

## **Assurances**

- 28 It is my opinion that NWFRA has adequate and effective control processes to manage its achievement of the Authority's objectives for the 12 month period to 31<sup>st</sup> March 2018. In reaching this opinion the following factors were taken into consideration:
- Internal Audit undertakes follow up action within six months of the issue of the final report in respect of audit assignments. The purpose of the follow up review is to determine the timeliness and effectiveness of the implementation of recommendations made to management. The follow up review process indicates that management have implemented or are in the process of implementing all of the recommendations made in our audit reports relating to 2016/17.
  - A schedule giving an audit opinion of the adequacy and effectiveness of control processes in respect of all the audit assignments undertaken during the year is attached at Appendix A. All audits undertaken during the year were assessed as providing positive levels of assurance, with the exception of the audit of Cyber Security, which provided a Limited level of assurance. The audit is scheduled to be followed up early in 2018/19.
- 29 The overall audit opinion may be used in the preparation of the Annual Governance Statement.

## **ANALYSIS OF WORK UNDERTAKEN AND DEFINITION OF AUDIT RECOMMENDATIONS AND OPINIONS**

- 30 The schedule at Appendix A details the conclusions and key messages of the assignments Internal Audit has reported upon during the year. The categorisation of recommendations informs the audit opinion in respect of each audit. Subsequently, a summary of each audit opinion made during the financial year informs the process whereby the Head of Audit and Procurement Services is required to include an opinion on the overall adequacy and effectiveness of the Authority's internal control environment, in his formal annual report to the Audit Committee.

## Risk Ranking Categories

- 31 Audit recommendations are categorised to reflect the way in which the Authority assesses and measures risk. The standard risk assessment criteria are shown below:

LIKELIHOOD	Event is almost certain to occur in most circumstances	>70%	Almost Certain	A	Very Low	Low	Medium	High	Very High
	Event likely to occur in most circumstances	30-70%	Likely	B	Very Low	Low	Medium	High	Very High
	Event will possibly occur at some time	10-30%	Possible	C	Very Low	Low	Medium	High	Very High
	Event unlikely and may occur at some time	1-10%	Unlikely	D	Very Low	Low	Medium	High	Very High
	Event rare and may occur only in exceptional circumstances	<1%	Rare	E	Very Low	Low	Medium	High	Very High
					5	4	3	2	1
					Very Low	Low	Medium	High	Very High
Service Performance		Minor errors or disruption	Some disruption to activities/customers	Disruption to core activities/ customers	Significant disruption to core activities. Key targets missed	Unable to delivery core activities. Strategic aims compromised			
Reputation		Trust recoverable with little effort or cost	Trust recoverable at modest cost with resource allocation within budgets	Trust recovery demands cost authorisation beyond existing budgets	Trust recoverable at considerable cost and management attention	Trust severely damaged and full recovery questionable and costly			
Financial	Cost (£)	<£50k	£50k - £350k	£350k - £1 m	£1 m - £5 m	>£5m			
<b>IMPACT</b>									

### Severity



Minor



Moderate



Major



Critical

### Management Intervention

Findings which are easily addressed by line management.

Findings that identify non-compliance with established procedures but do not represent any major risk to the Authority, containable at service level.

Important findings that need to be resolved by Principal Officers and Executive Panel may need to be informed.

Findings that are fundamental to the management of risk in the business area, representing weaknesses in control that require the immediate attention of the Executive Panel.

## Audit Opinion

- 32 The outcome of each audit and the evaluation of the adequacy of the internal control environment is based on the number of recommendations made and their risk rating. This process informs the Audit Opinion and the following definitions have been produced to enable auditors to make appropriate assessments in respect of the Audit Opinion contained at the end of each audit report.

### DEFINITIONS OF ASSURANCE RATINGS

LEVELS OF ASSURANCE	CONTROLS	RISKS
<b>HIGH ASSURANCE</b>	Key controls are in place to ensure the achievement of service objectives and to protect the Authority against significant foreseeable risks and are applied consistently and effectively. No significant or material errors were found.	Low priority actions required which are easily managed.
<b>SATISFACTORY ASSURANCE</b>	Key controls exist to enable the achievement of service objectives and to mitigate against significant foreseeable risks. However, there was some inconsistency in application and opportunities still exist to mitigate further against potential risks.	Some opportunities still exist to mitigate further against potential risks.  Some risk of loss, fraud, impropriety or damage to reputation.
<b>LIMITED ASSURANCE</b>	Key controls are in place and to varying degrees are complied with but there are gaps in the process which leave the service exposed to risks. Objectives are not being met or are being met without achieving value for money.	There is a need to introduce additional controls and/or improve compliance with existing ones, to reduce the risk exposure to the Authority. A high risk of loss, fraud, impropriety or damage to reputation.
<b>NO ASSURANCE</b>	Key controls are considered to be insufficient with the absence of at least one critical control mechanism. There is also a need to improve compliance with existing controls and errors and omissions have been detected.	Key controls do not exist and objectives are not met or are being met without achieving VFM. The Authority is exposed to very significant risk, which could lead to major financial loss, reputational risk of embarrassment or failure to achieve key service objectives.



## **Common Weaknesses**

- 33 There is no common factor that links the weaknesses identified as part of our internal work for 2017/18. The Cyber Security audit and the Limited level of assurance may be considered relevant in the preparation of the Annual Governance Statement.

## **OTHER MATTERS**

### **Qualifications to the Audit Opinion**

- 34 In giving an audit opinion, it should be noted that assurance can never be absolute. The most that the Internal Audit Service can provide to the Audit Committee is a reasonable assurance based upon the work undertaken in that year, that there are no major weaknesses other than those identified.
- 35 Qualifications to the Audit Opinion are set out in paragraphs 13 and 14. In addition, in arriving at our opinion, we have taken into account:
- the results of all audits undertaken during the year ended 31st March 2018;
  - the results of follow-up action taken in respect of audits from previous years;
  - whether any High or Medium category of recommendations have not been accepted by management and the consequent risks;
  - the effects of any material changes in the Authority's objectives or activities;
  - matters arising from previous reports to the Executive Panel or Audit Committee;
  - whether or not any limitations have been placed on the scope of internal audit;
  - the resource constraints placed upon Internal Audit that have impinged on the Service's ability to meet the full internal audit needs of the Authority;
  - what proportion of the Authority's internal audit needs have been covered to date.

### **Acceptance of Recommendations**

- 36 Management have accepted 100% of the recommendations made by the Internal Audit Service during the year. There are no Critical or Major category recommendations that we consider are not receiving adequate management attention. There are 8 Major recommendations made in the Cyber Security audit; a follow up is scheduled for early in 2018/19 and the outcome will be reported to Members.

## **Reliance Placed Upon Work by Other Assurance Bodies**

- 37 Internal Audit places some reliance on work undertaken by the Wales Audit Office, the Authority's external auditors, particularly in relation to the financial statements, risk management and corporate governance arrangements in drafting the annual reports and forming our annual opinion of the period.

## **Issues Judged Relevant to the Statement on Internal Control**

- 38 Based on the work of the Internal Audit Section during 2017/18 it is considered that the results of Cyber Security audit and the Limited level of assurance may be considered relevant in the preparation of the Annual Governance Statement.

## **Compliance with Internal Audit Standards**

- 39 Internal Audit employ a risk-based approach to determining the audit needs of the Authority at the start of the year and use a risk based methodology in planning and conducting our audit assignments. The work of Internal Audit Services has been performed in compliance with the UK Public Sector Internal Audit Standards 2013.
- 40 Internal Audit is subject to annual review by External Audit to determine compliance with the UK Public Sector Internal Audit Standards 2013.
- 41 The Public Sector Internal Audit Standards (PSIAS) became effective from 1<sup>st</sup> April 2013 and introduced a requirement for an external assessment of all internal audit services, which must be conducted at least once every five years by a qualified, independent reviewer from outside of the organisation. Wrexham County Borough Council's (WCBC) Service Manager – Audit and Technical performed the assessment in November 2016. The Institute of Internal Auditor's suggest a scale of three ratings, 'Generally Conforms,' 'Partially Conforms', and 'Does Not Conform.' The external assessors' overall opinion is that the Internal Audit Service generally conforms with the PSIAS and Code of Ethics in all significant areas and that it operates independently and objectively.
- 42 The Head of Internal Audit has made provision for internal quality reviews to be undertaken periodically by experienced members of the internal audit function to appraise:
- compliance with the organisational and professional standards,
  - the quality of audit work and supervision,
  - compliance with the local audit manual,
  - the achievement of performance indicators.

- 43 The review conducted in respect of the work performed during 2017/18 has demonstrated compliance with both internal and external standards.

### **Internal Quality Assurance Programmes**

- 44 In order to ensure the quality of the work performed by Internal Audit, a range of quality measures are in place which include:
- supervision of staff conducting audit work;
  - documented review of all files of working papers and reports by managers;
  - an annual appraisal of audit staff resulting in personal development and training action plans;
  - the maintenance of the Section's Internal Audit Manual.

### **IMPLICATIONS**

Wellbeing Objectives	This report links to NWFRA's long-term well-being objective which is "To facilitate high quality, responsive and better integrated fire and rescue services so that prevention activity and emergency response can continue to be available when and where required, affordably, equitably and on the basis of risk."
Budget	Internal Audit Services is provided as part of an SLA and within budget constraints.
Legal	N/A
Staffing	N/A
Equalities/Human Rights/ Welsh Language	N/A
Risks	<p>The Statement of Assurance is submitted in compliance with the Accounts and Audit Regulations and the Public Sector Internal Audit Standards. Without such assurance from the Head of Internal Audit Services, Members would be unaware of the adequacy and effectiveness of the corporate governance, risk management and internal control arrangements and its associated ability to achieve its objectives.</p> <p>Any significant issues or weaknesses identified by Internal Audit would not be considered in the preparation of the Annual Governance Statement.</p>

**NORTH WALES FIRE AND RESCUE AUTHORITY**

**APPENDIX A**

**Internal Audit Section – 2017/18 Annual Summary of Recommendations and Audit Opinions**

	<b>Auditable Area</b>	<b>Audit Findings and Key Messages</b>	<b>Critical</b>	<b>Major</b>	<b>Moderate</b>	<b>Minor</b>	<b>Total</b>	<b>Agreed by Mgmt</b>	<b>Audit Opinion</b>
1	<b>Cyber Security (Part 1)</b>	<p>Cyber security consists of a mixture of technologies, processes and measures that are designed to protect systems, networks and data from cyber-crimes, reducing the risk of a cyber-attack and protecting the organisation and individuals. Security grows out of doing things properly across the board and making sure that people at all levels understand the threats to the whole organisation. A cyber-attack is usually intended to inflict damage or obtain information from an individual, organisation or public entity for the purpose of theft, unauthorised access to networks, compromise of official records or financial and/or reputational damage.</p> <p>The risk of a cyber-attack is included on NWFRS's risk register, staff at all levels within the organisation and executive management are routinely made aware of the current situation in relation to Cyber Security and threats, etc. There are Service Administration Policy and Procedure Orders (SAPPOs) in place, but these need to be reviewed in a timely manner and rolled out to the workforce to ensure they accurately reflect a constantly evolving area. In addition, whilst there is some data protection training available and a presentation has been established, this needs to be rolled out and the workforce encouraged to attend or complete the online training, which includes some guidance and best practice in relation to data security. Reactive training and notifications were evident to warn of potential attacks and this along with the proactive software raises staff awareness, however, the updating of SAPPOs, conclusion of Information Security training and the implementation of cyber security/defence training, aligned with job role, will encourage and maintain a security conscious culture within NWFRS and reduce the risk of a successful attack, especially via social engineering techniques.</p> <p>Cyber crime risk intelligence and threat advisories are received from a number of sources, but due to the volume of advisories and vulnerability patches received this area requires further consideration, to ensure that the notifications are reviewed timely and any necessary action taken. When patches and software updates are provided by vendors the release notes are usually published on the internet, providing a wealth of information for individuals wishing to take advantage of any vulnerabilities that the updates will address, therefore it is essential that the ongoing</p>	0	8	9	1	18	18	Limited

	Auditable Area	Audit Findings and Key Messages	Critical	Major	Moderate	Minor	Total	Agreed by Mgmt	Audit Opinion
		<p>discussion between NWFRS and 3TC regarding the prompt application of windows updates on the Guardian Command and Control network are concluded and that vendor supplied patches or software updates that contain critical or security updates are applied in a timely manner, to reduce the risk of successful attack via this means.</p> <p>Separate ICT and Command and Control Business Continuity Plans are in place and resilience is tested as a matter of routine and via naturally occurring events. Network diagrams were evident, which appeared to be up to date and whilst a spreadsheet has been established as a basis for the Information Asset Register, this is yet to be populated and a Data Classification scheme is not in place. Issues surrounding the recording of the hardware and software assets also need to be resolved to ensure all asset records provide a comprehensive, accurate picture of the assets held, thus enabling their criticality to the organisation and the risk to the assets from threats and known vulnerabilities to be appropriately assessed and sufficient controls applied.</p> <p>Change Control can help to safeguard and reduce the risk of unnecessary errors and service disruption or downtime to IT services and the implementation of a formal Change Management process would provide assurance that the change and any repercussions have been considered appropriately and the process for implementation, back out and lessons learnt are appropriately managed, this is increasingly important given the limited staff resources in the ICT department.</p> <p>Laptops and tablets are configured from a standard image and BitLocker encryption is applied. Egress is available to secure any business sensitive data sent via email. System users are prevented from installing or disabling software/applications/security settings via group policy and through the local permissions applied to them and the use of mobile storage devices is controlled by policy and technically enforced. Vendor supplied default user accounts were identified, but assurance was provided that the passwords had been amended. Privileged access that is unrestricted, enabling full access across the whole infrastructure is provided to a number of individuals via group policy, but there is minimal auditing and logging of the tasks performed by a privileged user. In order to limit the impact of any compromise, whether intentionally or in error, via a privileged user account, this level of access needs to be reviewed and provided on a least privileged basis, i.e. tailored to the roles undertaken. The conclusion of ongoing work to move the management of mobile devices to AirWatch and the supporting</p>							

	Auditable Area	Audit Findings and Key Messages	Critical	Major	Moderate	Minor	Total	Agreed by Mgmt	Audit Opinion
		SAPPO will reduce the risk of data being accessed by unsecured lost, stolen or misplaced devices.							
2	<b>Retained Stations (Conwy &amp; Denbighshire)</b>	<p>The audit review indicates that generally there are a number of areas within Conwy &amp; Denbighshire's Retained Fire Stations and associated systems that appear to be working well with key controls in place. It was confirmed that the electronic FIN8 System is operating effectively; FIN8s accurately record the incident number, times of alert and dismissal, attendances, quarters, drills etc., payment data is accurately transferred to the payment schedules and firefighters are correctly paid for any fees and allowances they are entitled to. However, it was identified that an overpayment of £2,173 was made to FFD (81925) in October as a result of an inputting error into the Standing Data Spreadsheet (Sept 17 Claim). It is acknowledged that the overpayment was identified prior to the audit and the monies recovered by cheque from the firefighter in October. An overpayment of £16.14 was also made to FFD (81640) in October as 3 days holiday leave were paid at a daily rate of £13.04 and not £7.64 as a result of an inputting error on Standing Data Spreadsheet. Audit tests identified two minor errors in the transfer of data from the Attendance Registers to the associated FIN 8, by the respective watch managers, which resulted in an underpayment of £10.67 to a firefighter.</p> <p>The National Fire Cadets is an educational youth organisation, which provides an opportunity for young people between 13 and 18 to achieve national recognised qualifications, with branches at Amlwch, Beaumaris, Conwy, Chirk, Llanfairfechan, Prestatyn and Pwllheli. It was identified during the Station visits and attendance register checks (Sept 2017) that an Instructor (81668) has not had an Enhanced DBS check. The Deputy Head of Community Safety maintains a list of Cadet Instructors and whether Enhanced DBS checks have been completed. It was identified that there are currently 5 instructors (inc.81668) who have not had Enhanced DBS checks as they have not returned the application form and proof of ID. It was confirmed that if any Lead Instructors have not had an Enhanced DBS Check by 31/1/18 they will be prevented from working as an Instructor, with DBS checks on Lay Instructors completed by 31/3/18.</p> <p>It was confirmed that an Order (<i>SAPPO Premises Inventory Policy</i>) is in place to detail the expected procedures for safeguarding the Service's</p>	0	1	1	7	9	9	<b>Satisfactory</b>

	Auditable Area	Audit Findings and Key Messages	Critical	Major	Moderate	Minor	Total	Agreed by Mgmt	Audit Opinion
		<p>assets; retained stations are utilising official premises inventory books (PIB) and the annual checks are signed and dated by the officer responsible. However, the PIB has been lost at Conwy Retained Station and the prescribed annual checks have not been undertaken at Llanfairfechan and St Asaph since 2014 and at Betws y Coed since 2015. In addition, the Locality Manager is not complying with the SAPPO and undertaking annual audits of the PIB for Stations under their command.</p> <p>It was confirmed that in accordance with the SAPPO, fire appliance inventory checks are being undertaken at Conwy &amp; Denbighshire Retained Stations at least on a weekly basis on drill nights. Watch Managers are generally undertaking the quarterly verification checks, however, the WM checks have not been performed at Llanfairfechan &amp; Ruthin since 2016. With the exception of Prestatyn Station, the 6 monthly Locality Manager verification checks have not been performed since 2014 &amp; 2015 and the Operations Department are not completing the annual quality assurance audits.</p> <p>It was confirmed that each vehicle maintains a log book, which records the milometer readings, the refuelling of the vehicle, the signature of the driver after every journey and the signature of the supervising officer. In accordance with the SAPPO, the top copy of the log sheets are submitted to the Fleet Department at the end of each month.</p> <p>In relation to Welfare Funds it was confirmed that the Finance Section maintain a central record of Stations that operate welfare funds and on an annual basis request that treasurers submit audit certificates. At the date of the audit there were 4 Stations (1 Day Crewed, 1 Wholetime &amp; 2 Retained Stations (Menai Bridge &amp; Pwllheli) that had not submitted their annual audit certificate.</p>							
3	<b>Whistleblowing Policy &amp; Procedures</b>	<p>The Public Interest Disclosure (Whistleblowing) and Bribery Policy (SAPPO Section 7 Order 20) was issued in October 2014. The Policy includes the main criteria that should be included in a whistleblowing policy, although it should also include how employees can raise concerns outside the Service if dissatisfied with the response eg. to an external auditor, regulator or ombudsman. In addition, although the Policy does state that it is the responsibility of the HR Department for the content, issue &amp; any further amendment of the Order, it does not clearly identify a <i>Whistleblowing Policy Manager</i>, who has day to day responsibility for whistleblowing arrangements and the overall effectiveness of the Policy; the Policy is unclear &amp; ambiguous</p>	0	0	0	12	12	12	<b>Satisfactory</b>

	Auditable Area	Audit Findings and Key Messages	Critical	Major	Moderate	Minor	Total	Agreed by Mgmt	Audit Opinion
		<p>in places with regard to how the Service will respond to disclosures.</p> <p>The Support Services Co-ordinator emailed <i>All Uniformed Staff; Non-Uniform Staff; COAT</i> in October 2014, identifying that the SAPPO was in the Public Folders and on the NWFRS Intranet. However, it is considered that the Policy and guidance should also be available on the Service's website to facilitate external access for employees and to provide <u>contractors &amp; suppliers</u> access to the Policy.</p> <p>Whistleblowing &amp; Bribery Act training was provided to the Service by employment law specialists (VWV). Area Managers, group managers and heads of departments had completed the training by the end of January 2015 and it was arranged for as many line managers as possible to receive the training by the end of March 2015. Although the ACFO suggested at the time that the training could be provided to managers who were unable to attend the training and new managers via <i>Learnpro</i> (LMS) e-learning module, this initiative has not been progressed.</p> <p>The Service's whistleblowing procedures should encourage individuals to disclose concerns and it is crucial that awareness of the Policy is included in the Service's <i>Weekly Brief</i> or the quarterly newsletter <i>Y Fflam</i>. It has been found that it is new employees that are those most likely to raise concerns and reading &amp; understanding the Whistleblowing Policy should be included in the Employee Induction Programme. In addition, there may be times when an employee feels unable or unwilling to discuss concerns with immediate management and alternative channels inside the Service should be offered, such as a direct telephone line connected to an answer machine or a dedicated and confidential email address.</p> <p>The HR Manager identified that the only whistleblowing disclosures, since the inception of the Policy in 2014, have been raised after termination and dealt with via other policies or Employment Tribunals claims; as a result it has not been possible to test the Service's compliance with the Policy and best practice. However, a number of recommendations have been made for consideration, to ensure that appropriate procedures are in place. The Service should maintain a central record of whistleblowing disclosures and allocate disclosures with a unique reference number. In accordance with the Policy, disclosures should be responded to with 10 days, acknowledging that the concern has been received, how it proposes to deal with matter, an estimate of how long it will be to provide final response and an indication of whether further investigations will take place, and if not why</p>							



SWYDDOGOL-SENSITIF / OFFICIAL-SENSITIVE

	Auditable Area	Audit Findings and Key Messages	Critical	Major	Moderate	Minor	Total	Agreed by Mgmt	Audit Opinion	
		<p>not. Similarly all Whistle blowers should be written to within 10 working days after completion of the investigation to confirm the outcome of the investigation and indicate what further action will take place, and if not why not.</p> <p>Senior management &amp; Members need to consider the effectiveness of whistleblowing policies and procedures as part of their oversight of the system of internal control. Reports should be submitted on an annual basis to the Executive Group &amp; FRA, identifying the number of disclosures, the investigation outcome, feedback provided and any key control weaknesses.</p>								
4	NFI 2016/17	<p>NFI is a comprehensive and thorough 'data matching' exercise organised by the Cabinet Office in partnership with the Wales Audit Office (WAO). There were no issues arising from the investigations, which provides a level of assurance that the systems of internal control are working well and that frauds and irregularities are being minimized. The exercise also assists to strengthen anti-fraud &amp; corruption arrangements &amp; instil an anti-fraud culture.</p>	0	0	0	0	0	0	High	
									High	1
									Satisfactory	2
									Limited	1
									No Assurance	0

	Auditable Area	Audit Findings and Key Messages	Critical	Major	Moderate	Minor	Total	Agreed by Mgmt	Audit Opinion
--	----------------	---------------------------------	----------	-------	----------	-------	-------	----------------	---------------

## APPENDIX B

**NORTH WALES FIRE AND RESCUE AUTHORITY**  
**Schedule of Follow up Audits 2017/18**

	Description	Auditor	Audit Date	Follow up Due Date	Follow up Date	No. Recs	Recs Out-standing	Revised Audit Opinion
1	*NWFRS – Attendance Management	KVW	Dec-16	June-17	Oct-17	4	2	Satisfactory Assurance

**\*Note 1**

4 recommendations were made in the audit report issued in December 2016, 2 recommendations have been implemented and 2 of the recommendations are considered to be partially implemented. It was confirmed that the *Attendance Management Policy and Procedure* was approved by the Executive Group in September 2017. In addition, audit tests confirmed that the use of trigger points to manage attendance is now more consistently applied in accordance with the Policy and in all instances a review meeting had been held and the relevant warning issued at the defined trigger point.

In relation to the recommendations considered to be partially implemented, the following was identified:

Recommendation 2 required senior management at the start of each year to set sickness absence estimates / targets for each occupational group to enable performance to be measured and improved; and the performance target and actual data to be reported to the Executive Group and Members. The HR Manager produced an advisory paper for the DCFO identifying some options regarding absence rate formulas used in order to produce a target; the DCFO approved the CIPD Local Government (1.4) benchmark of **10.5** mean average days lost per employee per year. However, this excludes Retained Duty Station (RDS) sickness data as it was considered that absence may be measured more accurately by the Service using its own formula; at the time of the follow up a sickness absence target has not been set for RDS. It is also evident that a target has not been set for each occupational group; it is considered that since there is such a variance in the number of days/shifts lost per occupational group eg. 2016/17 Wholetime firefighters – 9.76 days & Non-Uniformed Personnel 19.93 days, that using the CIPD benchmark as a target is not an effective method of enabling performance to be measured and improved. It is considered that sickness absence targets should be set for each occupational group at the start of each year and actual data reported to the Executive Group to enable performance to be measured & improved.

Recommendation 3 required HR to provide further training and guidance to Station Watch Managers to ensure that they are aware of the requirements of the revised *Attendance Management Policy* and particularly the requirement for paperwork such as medical certificates and self-certification forms to be submitted to HR within 10 calendar days. The follow up has confirmed that the AM Policy has been approved and is available to staff on the Intranet; a further guidance document entitled *Attendance Management Policy Guidance 2017* is at the draft stage and it is important that this is issued as soon as possible to provide additional guidance. A programme of Station visits is in progress to enable the Senior HR Advisors to provide Watch Managers with additional training upon compliance with the Policy. However, audit tests performed upon 5 retained firefighter periods of absence, identified that only one medical certificate and one self-certification form, were received by HR within 10 days; two of the self-certification certificates have still not been received despite the firefighters returning to work in early August and repeated reminders. This indicates that despite the efforts of HR there are still significant issues with Watch Managers not promptly submitting sickness absence paperwork within approved timescales.

The previous audit report provided a Satisfactory level of assurance in respect of the operation of key controls and management of risk. The audit review and evaluation of the internal control environment is based on the number of recommendations made together with their risk rating. It is considered that the audit opinion in respect of NWFRS Attendance Management **remains as providing a Satisfactory level of assurance.**

**North Wales Fire and Rescue Authority  
Summary of Internal Audit Activity 2017/18**

	Department / Service	Planned Days 2017/18	Actual Days 2017/18
1	Main Financial Systems - <b>Creditors</b>	11	0
2	Cyber Security (Part 1) – Completion of audit Cyber Security (Part 2) – Audit Programme & Preparation	12	7
3	Retained Stations (Conwy & Denbighshire)	11	11
4	Whistleblowing Policy & Procedures	0	9
5	National Fraud Initiative (NFI)	7	8
6	Investigation into the Use of Service Vehicles – Private journeys, HMRC rules & taxable benefits in kind.	0	6
7	<b>Audit Follow ups:</b> • Attendance Management	7	4
8	NWFRA Planning & Reporting (Including Annual Report & Strategic Plan)	5	5
9	Contingency Reserve	2	0
	<b>TOTAL DAYS</b>	<b>55</b>	<b>50</b>
	<b>Days Allocated 2017/18</b>		<b>55</b>
	<b>Actual Days 2017/18</b>		<b>50</b>
	<b>Total Days C/F to 2018/19</b>		<b>5</b>

**North Wales Fire and Rescue Authority  
Draft Internal Audit Annual Plan 2018/19**

Needs Ass't Ref	Audit Review	Comments	Days	Planned Timing
<b>Risk Area – Financial and Fraud Risks</b>				
28	Main Financial Systems - <b>Creditors</b>	The ordering and payment for works, goods & services through Conwy's P2P System to ensure appropriate levels of internal control.	10	Dec 2018
25 & 28	Retained Fire Stations (Ynys Mon & Gwynedd)	Payment of salaries and allowances to firefighters on the retained duty system, the safeguarding of assets and maintenance of station and appliance inventory records, the recording of all journeys / refuelling in vehicle log books and the annual audit of Welfare Funds.	10	Sept 2018
23 & 28	Debtors	To review the Service's policy & procedures for the raising of debtor invoices, amendments to invoices, payments, debt recovery, write-offs and monitoring & reporting.	9	Feb 2019
<b>Risk Area – Information Management &amp; Technology</b>				
32	Cyber Security (Part 2)	The objective of the review is to provide management with an independent assessment relating to the effectiveness of cybercrime prevention, detection and incident management processes, policies, procedures and governance activities.	12	August 2018
<b>Other Audit Work</b>				
-	Audit Planning, Annual Report and Management	Provision for time required for management element of contract.	5	Ongoing
-	Follow up of Previous Recommendations	Following up recommendations made in 2017/18 – <ul style="list-style-type: none"> <li>• Cyber Security (Part 1)</li> <li>• Whistleblowing Policy &amp; Procedures</li> </ul>	7	Ongoing
-	Contingency Reserve	For unplanned work identified during the year and liaison/advice as required.	2	
<b>Total Days Required for Audit Work</b>			<b>55</b>	
<b>Total Days Allocated 2018/19</b>			<b>50</b>	
<b>Totals Days b/f from 2017/18</b>			<b>5</b>	
<b>Total Days Available 2018/19</b>			<b>55</b>	