Item 5

Staffordshire County Council

Staffordshire Fire and Rescue Service
preventing • protecting • responding

Staffordshire Commissioner Fire and Rescue Authority

INTERNAL AUDIT PROGRESS REPORT

5th February 2020
Report to the Ethics, Transparency and Audit Panel

Our Mission

To enhance and protect organisational value by providing risk-based and objective assurance, advice and insight.

Table of Contents

Contacts

Deborah Harris

Interim Chief Internal Auditor

01785 276406

deborah.harris@staffordshire.gov.uk

Alexander Cannon

ICT Audit Manager

01785 895334

alex.cannon@staffordshire.gov.uk

Internal Audit Service
Staffordshire County Council
2nd Floor, 1 Staffordshire Place
Tipping Street
Stafford
ST16 2DH

Introduction

This report presents the progress made against the Internal Audit Annual Plan for 2019/20 in addition to providing an update for the Ethics, Transparency and Audit Panel (ETAP) on Internal Audit activity since the last meeting held on 11th December 2019. It also provides information on the progress against recommendations made to the Fire & Rescue Service by Internal Audit.

Internal Audit reviews culminate in an opinion on the assurance that can be placed on the effectiveness of the framework of risk management, control and governance designed to support the achievement of management objectives of the service area under review. Assurance opinions are categorised as follows:

- **Substantial Assurance (positive opinion)** - We are able to offer substantial assurance as the areas reviewed were found to be adequately controlled. Internal controls were in place and operating effectively and risks against the achievement of objectives were well managed.
- **Satisfactory Assurance (positive opinion)** - We are able to offer satisfactory assurance as most of the areas reviewed were found to be adequately controlled. Generally, risks were well managed, but some systems required the introduction or improvement of internal controls to ensure the achievement of objectives.
- **Limited Assurance (negative opinion)** - We are able to offer limited assurance in relation to the areas reviewed and the effectiveness of the controls found to be in place. Some key risks were not well managed and systems required the introduction or improvement of internal controls to ensure the achievement of objectives.

2019/20 Audit Plan Progress

Audit Name	Status	Assurance
General Audits		
Police – Fire Collaboration	Draft Report Produced	
Fire Fighters Pensions administration & Pensions Payroll*	Being Reviewed	
Budgetary Control, Financial Monitoring & Reporting	Cancelled	
Health and Safety ***(New)***	Planning – Fieldwork commencing w/c 02/03/20	
Financial Ledger & Bank*	Planning – Fieldwork commencing 17/2/20	
Payroll Processing Procedures*	Planning – Fieldwork commencing 21/2/20	
Insurance Arrangements	Final Report Issued	Satisfactory
ICT Audits		
Firewatch – Application Audit	Final Report Issued	Satisfactory
Cybersecurity – Patch Management	Final Report Issued	Substantial
Anti-Fraud Culture		
Fraudwatch Publication	Planning	N/A
Detection		
National Fraud Initiative 2018	In progress	
Development and undertaking of Data Analytics	Cancelled	
Prevention		
Fraud Risk Assessment	Cancelled	N/A
Fraud and Corruption Checklists	*Completed as part of the above systems audits	

Since the last ETAP meeting in December 2019, Cybersecurity Patch Management audit has been finalised. A substantial assurance opinion was awarded with 1 medium recommendation and 3 low priority recommendations being made. The management summary for this audit can be found in **Appendix 1**. The draft Internal Audit report for the Police – Fire Collaboration audit review has also been produced and a closing meeting is to be arranged with Police and Fire Management to discuss the findings of this audit.

Adjustments to the Internal Audit Plan

The following changes have been made to the 2019/20 Internal Audit plan with agreement from the Director of Finance (Staffordshire Commissioner's Office)/S151 Officer:

- At the request of the Director of Finance (Staffordshire Commissioner's Office)/S151 Officer, the Budgetary Control, Financial Monitoring & Reporting audit has been cancelled. Instead, assurance will be taken from Staffordshire Fire & Rescue Service's own internal scrutiny arrangements in place during 2019/20 to monitor and report upon budgets across the organisation. The Budgetary Control, Financial Monitoring and Reporting audit has been replaced by a Health & Safety audit review due to (i) the time that has passed since this area was last reviewed; and (ii) a serious Health & Safety incident has occurred during the year.

- The Development and Undertaking of Data Analytics work has been cancelled due to a lack of value in delivering this work now given the imminent changes to your Internal Audit provider. The main objectives for this year was the development of data governance procedures and tests which can then be applied in following years to allow for greater data analysis and enhanced assurance in a fraction of the time. However, as SCC will no longer be providing Internal Audit services post 31st March 2020, there is little value to either parties in developing this area.

- The Fraud Risk Assessment is completed during the annual planning process. However, as SCC Internal Audit Service will no longer be providing Internal Audit services post 31st March 2020, no planning or risk assessment is required for 2020/21.

The time originally allocated to the data analytics work and the fraud risk assessment totalling 8 days, has been re-assigned to the Police – Fire Collaboration audit review where 21 days have been used to date (against an original time budget of 13 days).

Audit Recommendations

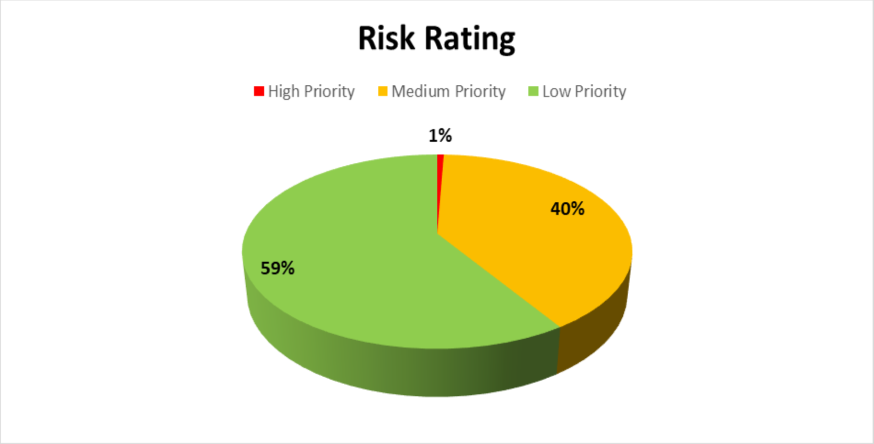
As part of Internal Audit's service to the Staffordshire Fire and Rescue Service, we record, monitor and report on all recommendations that have been made in our audit reports.

Risk Rating

Each recommendation that we make is risk assessed, and based on an assessment of likelihood and impact, 1 of the 3 following priority levels will be awarded:

- High Priority
- Medium Priority
- Low Priority

Since the implementation of an Audit Management System in 2016 which is used to monitor all recommendations, a total of 175 recommendations have been imported for monitoring and reporting. Of these recommendations, 1 is a high priority, 65 are a medium priority and 109 are a low priority.



Action Status

Each recommendation that is imported into the Audit Management System is allocated a responsible officer and an agreed action date, which are detailed in the internal audit's final report. Once this agreed action date has passed, an email is sent to the responsible officer asking them to provide an update on the progress made against the recommendation.

Following this response, the recommendation is given a status to enable us to monitor and categorise the progress of recommendations. The following status' can be assigned to a recommendation:

- **Implemented** – Audit have been informed that the control weakness has been addressed.
- **Partially Implemented** – Audit have been informed that the agreed action is a work in progress, some elements may have been implemented.
- **Outstanding** - Action has been agreed upon with management but is yet to be implemented.
- **Deferred** - The agreed actions have been deferred until a later date (e.g. it may be dependent on another activity, action or upgrade).
- **Superseded** – Audit have been informed that the control weakness no longer exists due to changes in the system or business process.
- **Risk Accepted** – Management accept the risk and no mitigating action will be taken to address the control weakness identified.

Recommendations Summary

The table below summaries the status for each recommendation made to the Staffordshire Fire & Rescue Service. No recommendations have been implemented since the last ETAP meeting.

		Implemented	No Action to be Taken		Not Yet Implemented			Agreed/Revised Action Date	
Priority	Recs Made	Implemented	Superseded	Risk Accepted	Deferred	Partially Implemented	Outstanding	Not Overdue	Overdue
High	1	1	0	0	0	0	0	0	0
Medium	65	56	0	1	2	2	4	4	4
Low	109	87	2	2	2	0	16	10	8
TOTALS	**175**	**144**	**2**	**3**	**4**	**2**	**20**	**14**	**12**

Overdue Recommendations

Of the 175 recommendations that Internal Audit are tracking, 26 have yet to be implemented with 12 having passed their agreed or revised action date. A summary of these recommendations is shown below with further detail being shown in **Appendix 2**.

Audit	Priority	Control Issue	Agreed Action Date	Revised Action Date
Firewatch Application Review	Medium Priority	A Firewatch integration Team has been established to manage and develop Firewatch in a business as usual environment. However, the project has not been formally closed.	30/09/2017	31/12/2019
Firewatch Application Review	Medium Priority	Although a range of benefits achievable from the project were noted in the PID and more have since been identified by staff involved in the project, a benefit realisation plan has not been prepared.	30/09/2017	31/12/2019
Fire Fighters Pensions Administration and Payroll	Low Priority	There is a 3-year gap between disaster recovery testing being performed. This does not provide up to date assurance that the pensions administration system can be reconstructed if required.	01/06/2019	31/01/2020
Fire Fighters Pensions Administration and Payroll	Medium Priority	The level of the contractors delegated authority has not been documented.	01/07/2019	31/01/2020
Cybersecurity Preparedness and Response effectiveness	Low Priority	SFRS have not documented what can or cannot be done to limit the potential for a cyber incident with their current resources and budget.	31/12/2019	-
Integra - System Security	Medium Priority	Whilst the Fire Service conducts annual health checks against the externally facing firewall of Integra, no penetration test is completed of the hosted solution.	31/07/2019	31/12/2019
Integra - System Security	Low Priority	The business impact assessment does not consider timescales.	31/07/2019	-

Firewatch	Low Priority	Procedural guidance had not been produced to support the process to restore data from back-ups.	31/01/2020	-
Firewatch	Low Priority	A report confirming success of the back-ups, sent to the ICT team was not being evidenced by the person performing the check.	31/01/2020	-
Firewatch	Low Priority	It was possible to access, complete and submit an Action Slip via the staff intranet which was not in adherence to proper practice.	31/12/2019	-
Firewatch	Low Priority	Checks on large scale inputs to Firewatch in terms of uploads of leave entitlements were being undertaken, but these were not being evidenced.	31/01/2020	-
Firewatch	Low Priority	Absence data was being manually transferred from Firewatch for manipulation within a spreadsheet by HR to track staff reaching trigger points defined by the Absence Management policy.	31/01/2020	-

Appendix 1

FINAL Report

Cybersecurity – Patch Management

1 Executive Summary

1.1 Scope and Background of Audit

1.1.1 The audit reviewed five key areas: policy and procedure; information security function and responsibilities; patching is undertaken in a controlled and methodical manner; remedial action; and KPIs.

1.1.2 Patch Management is the process of updating software and firmware on IT devices, to improve usability and security. Software providers regularly release updates to address functionality issues as well as known security vulnerabilities. External threats such as hackers, use these vulnerabilities to gain access to organisations' systems and data. Patch management is one of the key hygiene processes to protect an organisation from vulnerabilities in their systems, which can then be exploited by hackers. Therefore, it is essential that organisations have a robust patch management regime to adequately protect themselves, combined with other security measures such as firewalls.

1.1.3 This audit focused on the patch management processes within SFRS, where systems are maintained and supported by the IT Team. This covers Windows desktops, Windows servers, SQL servers, and network/communications equipment. The patch management of individual systems and applications owned by business units was not included in the scope of this review.

1.2 Summary of Audit Findings

Control Objectives Examined	No of Controls Evaluated	No of Adequate Controls	No of Partial Controls	No of Weak Controls
Clearly defined policies and procedures have been developed and are operational in order to support a structured approach to patch management. Furthermore, roles and responsibilities have been clearly defined and communicated.	1	1	0	0
An information security function has been established that has responsibility for patch management. All involved in the Patch Management process have undergone adequate training.	1	1	0	0
Patching is undertaken in a controlled and methodical manner following defined procedures. Patch criticality should be evaluated and only the latest stable tested releases of software should be deployed in a structured manner, with adequate regression testing prior to deployment.	1	0	0	1

Appropriate remedial action is taken where vulnerabilities are identified. Processes exist for identifying vulnerabilities with critical vulnerabilities identified and mitigated within 48 hours of identification.	1	1	0	0
Appropriate KPI's are defined and are monitored in respect of applying security patches. The indicators are prioritised by risk and criticality.	1	0	0	1
TOTALS	**5**	**3**	**0**	**2**

1.2.1 The following issues were considered to be the key control weaknesses:

Rec Number	Risk Rating	Summary of Weakness	Agreed Action Date
1	Low Priority	Whilst the Policy provides an overview of the patching process, detailed procedures for each specialist area of patching have not been written.	30/06/2020
2	Low Priority	SFRS do not receive any management information from KComm to provide assurances that patches are being applied to networking and communications components.	30/06/2020
3	Medium Priority	The inventory/list of patch requirements are incomplete, therefore SFRS do not have a complete view of the patching environment.	31/03/2020
4	Low Priority	KPIs and KRIs are not defined, therefore management are not able to determine that minimum defined targets are being met, or whether performance is improving or deteriorating.	30/6/2020

This report focuses on the weaknesses in the Organisation’s systems of control that were highlighted by this audit and recommends what Audit considers to be appropriate control improvements. This report contains the follow amount of recommendations

High	**Medium**	**Low**	**Total**
0	1	3	4

1.3 Summary of Control Assurance Provided

1.3.1 **Substantial -** Internal Audit are able to offer substantial assurance as the areas reviewed were found to be adequately controlled. Internal controls were in place and operating effectively and risks against the achievement of objectives were well managed.

2 Positive Assurance

We attempted to establish whether the Organisation's system of control for the following areas contained all the key controls expected of a sound and robust process. Through a combination of control evaluation and testing we confirmed that the following adequate controls were in operation:

2.1 Patching Policy

- The ICT Patching and Vulnerability Management Policy was approved by the Protective Security Steering Group (PSSG) on 23/10/2019.
- The policy sets out key roles and responsibilities and includes the main points as expected:
  - It clearly defines the scoring mechanism to determine the severity of the vulnerability, using a scale between 0 and 10 and categorised between Low to Critical. This is based on vulnerability scores published by the National Institute of Standards and Technology's National Vulnerability Database.
  - The policy also sets out the timescales of the patching process and end of life policy.
- The policy includes the date of issue and approval information. As the policy was only approved the day before the audit commenced, it was still to be updated with the Director/Manager approval.

2.2 Information Security Function

- Training budgets have been cut in recent years due to lack of funding. Where possible, training is provided internally. Patching responsibilities are also rotated on an annual basis if possible, to ensure all members of the team gain some experience in the different areas of patching.
- Where specialist skills do not exist within the team, 3rd party vendors are used to provide support.
- Given the small size of the team, it would not be practical for there to be a wide number of specialist staff, or for a few staff to have a wide range of specialisms. Therefore, the Head of ICT feels they have an appropriate balance which enables the IT team to deliver the service required, balanced with retaining staff, and cost of training.

2.3 Patching Procedures

- There is a systematic approach to patch management within SFRS. As outlined in the Policy, new patch releases are not implemented immediately, as there are often operational issues caused by the updates. This allows vendors time to recall faulty patches.
- For Windows operating systems, patches are rolled out to a pilot group within 7 days of release, which enables users and the IT team to identify any issues with the patch update. This limits the extent of any impact on operations and enables patch deployment to be reversed without a significant drain on resources. After the 7 days, if there are no issues, the remainder of the systems are patched within 14 days of the release date. For mobile devices and tablets, the patches are applied within 7 days of release. Evidence was provided to demonstrate a number of patch deployment policies in support of this as well as logs demonstrating that patches have been deployed within the specified timeframe.
- Windows patch releases are published on the 2nd Tuesday of each month (Patch Tuesday). Windows patches are bundled together, with no differentiation between

critical and non-critical. It is not practical to dissect the bundle into priorities to only install the critical patches. However, the current procedure adopted by SRFS is adequate to install the patches in a timely manner.

- For devices that are often disconnected from the network, such as laptops, patches are automatically pushed to the device the next time the device connects. The user can deny the update initially if they wish, but then the system forces the update to be applied within 48 hours of connection. This prevents the users from continually preventing patch and system updates.
- The Service Desk is automatically notified of devices not connected to the network for 30 days. An engineer then contacts the user and requests them to bring the device in.
- Exchange and SQL servers are updated quarterly due to the complexities involved and impact on end user operations. SFRS are moving away from on premise Exchange to Office 365, so this will not be a requirement in the future. SFRS are also moving to new SQL servers which will be easier to maintain, and patches will be applied monthly. Other servers are mostly rebooted weekly and patches are automatically applied where possible. Other systems, such as Firewatch, are patched manually as this system is required 24/7 and is done 7 days after Patch Tuesday.
- SRFS use a system called Manage Engine to roll out patches to Windows devices and 3rd party applications, this allows the patching of 3rd party applications such as Adobe.
- New builds must be run through the Nessus software, which is used to monitor vulnerabilities. This ensures that all new devices are recognised and monitored by this system and are not commissioned with vulnerabilities already existing.
- Mobile devices are managed by a system called Soti MobiControl. This enables all devices to be logged, monitored and updated as required.
- Patching does not generally go through formal change control procedures, unless it involves significant changes to the system or its configuration. If a highly critical patch requires installing, and it is outside of the normal schedule, this must be approved by the SIRO. Due to the small size of the IT team, members are generally aware of the current status of systems and any issues. The roll out to a trial group acts as a testing ground prior to main release, and patches can be uninstalled if required.
- SFRS gained Cyber Essentials accreditation in April 2019. Cyber Essentials includes a patch management technical control theme. This requires SFRS to patch software within 14 days of an update being released, where the patch fixes a vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’.

2.4 Remedial Action

- SFRS uses Nessus, alongside the Manage Engine system to identify where patches have not successfully been deployed. Action is taken to investigate why this might be, and appropriate action taken.
- SFRS are currently decommissioning Citrix. Some patches have not been applied over the past few months as a result, which has increased the number of reported instances of failed patching. However, prior to the Citrix decommissioning commencing, the number of critical patches outstanding was minimal. Most of the outstanding critical patches was due to the component no longer being supported by the vendor. Reports from June 2019 were reviewed.

Appendix 2

Overdue Audit Recommendations

1391	Firewatch Application Review				Report Issued	26/06/2017
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
1	Medium Priority	30/09/2017	31/12/2019	Deferred	4	Head of ICT

Control Issue

A Firewatch integration Team has been established to manage and develop Firewatch in a business as usual environment. However, the project has not been formally closed.

Recommendation

A Firewatch project closure report be prepared for Project Board approval. The report should:

- Assess whether go-live has been successfully achieved
- Assess whether the objectives of the project have been achieved within timescales and budget
- arrange for the treatment of residual risks and issues and on-going benefit realisation
- capture lessons learnt and allow for formal handover to the business as usual team.

Action Details

To mark the end of the formal project stage a project closure report will be produced and presented to the board.

Status Updates

Update received from Wil Lloyd 14/03/2019 - The project has been delayed further and it is anticipated that the recommendation cannot be completed until the end of the year.

Update received from Wil Lloyd 30/10/2018 - This is now delayed until January 19. I would expect the report to be compiled by end of Feb 2019

Update received from Wil Lloyd 19/6/18 - The production of a project closure report and benefits realisation has been deferred until version 7.6 of Firewatch is deployed later this year. This version includes updates to more efficiently support changes in the way the organisation operates its resourcing.

1391	Firewatch Application Review				Report Issued	26/06/2017
Rec Number	Rating	Action Date	Revised Action Date	Rec Number	Rating	Action Date
2	Medium Priority	30/09/2017	31/12/2019	1	Medium Priority	30/09/2017

Control Issue

Although a range of benefits achievable from the project were noted in the PID and more have since been identified by staff involved in the project, a benefit realisation plan has not been prepared.

Recommendation

Business benefits be formally identified, measured, tracked and plans made for their realisation.

Action Details

As part of the project closure report a benefits realisation report will be produced.

Status Updates

Update received from Wil Lloyd 14/03/2019 - The project has been delayed further and it is anticipated that the recommendation cannot be completed until the end of the year.

Update received from Wil Lloyd 30/10/2018 - This is now delayed until January 19. I would expect the report to be compiled by end of Feb 2019

Update Received from Wil Lloyd 19/6/18 - The production of a project closure report and benefits realisation has been deferred until version 7.6 of Firewatch is deployed later this year. This version includes updates to more efficiently support changes in the way the organisation operates its resourcing.

1872	Fire Fighters Pensions Administration and Payroll				Report Issued	24/04/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
11	Low Priority	01/06/2019	31/01/2020	Outstanding	8	Director of Finance

Control Issue

There is a 3-year gap between disaster recovery testing being performed. This does not provide up to date assurance that the pensions administration system can be reconstructed if required.

Recommendation

The Director of Finance, Assets & Resources should review the backup and disaster recovery arrangements with WYPF to determine whether the length of time between disaster recovery testing is acceptable. Appropriate action should be taken, as determined.

Action Details

This is to be discussed and reviewed with WYFP.

Status Updates

Advised by David Greensmith on 23/10/19 - The testing will be further delayed as West Yorkshire are installing new servers and will not be carrying out further testing until January 2020. However, assurance has been given that daily backups are taken.

1872	Fire Fighters Pensions Administration and Payroll				Report Issued	24/04/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
12	Medium Priority	01/06/2019	31/01/2020	Partially Implemented	7	Director of Finance

Control Issue

The level of the contractors delegated authority has not been documented.

Recommendation

The level of the contractors delegated authority should be agreed and documented, and processes should be in place to monitor the contractor's adherence to the powers that have been delegated to it.

Action Details

The delegations are being update and will be reported through the Strategic Governance Board

Status Updates

Advised by David Greensmith on 29/10/19 - some outstanding issues with the delegations remain that are being discussed with West Yorkshire.

Advised by David Greensmith on 23/10/19 - Delegated Authority, the authority is in place this just needs to be updated in relation to a couple of recent changes. The changes will be put through the Strategic Board on the 28 November 2019

1876	Cybersecurity Preparedness and Response effectiveness				Report Issued	23/04/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
2	Low Priority	31/12/2019	-	Outstanding	1	Head of ICT

Control Issue

SFRS have not documented what can or cannot be done to limit the potential for a cyber incident with their current resources and budget.

Recommendation

SFRS should review the level of maturity it has in cyber security incident response and compare it to its actual requirements for such a capability to highlight what can be achieved with existing resources.

Action Details

Desktop cyber event exercises being carried out over the current year will be used to identify the appropriate levels of resource required and available to the service and then documented

Status Updates

None

1877	Integra - System Security				Report Issued	02/04/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
3	Medium Priority	31/07/2019	31/12/2019	Outstanding	2	Head of ICT

Control Issue

Whilst the Fire Service conducts annual health checks against the externally facing firewall of Integra, no penetration test is completed of the hosted solution.

Recommendation

The Fire Service should consider commissioning an external penetration test against Integra by an independent 3rd party to gain assurance that Fire Service data is held securely within Integra.

Action Details

We will explore the option of penetration testing on the offsite Integra Server.

Status Updates

Update from Corrina Bradley 23/10/19 - the Head of ICT is carrying out a joint piece work with SCC, discussions are underway and hopefully there will be an update by the end of Dec.

Update from Corrina Bradley 8/7/19 - Patches are performed monthly as an ongoing activity by Capita hosting team. Service Delivery Manager to understand the documents they hold and the evidence they can produce (the procedure in place and the evidence of compliance). WL/CB to chase up capita.

1877	Integra - System Security				Report Issued	02/04/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
7	Low Priority	31/07/2019	-	Outstanding	2	Head of ICT

Control Issue

The business impact assessment does not consider timescales.

Recommendation

Management should consider including short, medium and long term effects within the risk assessment.

Action Details

A Business Impact Assessment will be carried out to consider the short term, medium term and long-term impact.

Status Updates

Update from Corrina Bradley 8/7/19 - Waiting for feedback from WL regarding BIA.

2138	Firewatch				Report Issued	04/12/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
3	Low Priority	31/01/2020	-	Outstanding	1	ICT Development Manager

Control Issue

Procedural guidance had not been produced to support the process to restore data from back-ups.

Recommendation

A set of procedural guidance notes should be produced in support of the process to restore the Firewatch system from back-ups recorded to tape and by snapshots of the system. These procedures should be tested on members of the ICT Team who do not usually perform these tasks to ensure business continuity and ensure resilience of this part of the service.

Action Details

ICT will produce a written procedural guidance note to reference the process for applying a database back up from LIVE into either the TEST or TRAIN systems.

Having produced the guidance this will be shared between members of the ICT team with experienced members providing opportunity and support for less experienced members to develop their knowledge in this area.

Status Updates

None

2138	Firewatch				Report Issued	04/12/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
4	Low Priority	31/01/2020	-	Outstanding	1	ICT Development Manager

Control Issue

A report confirming success of the back-ups, sent to the ICT team was not being evidenced by the person performing the check.

Recommendation

A control record should be introduced to allow officers checking the reports from Firewatch to evidence that they have viewed the information and when.

Action Details

System of work to be developed and implemented within the ICT team

Status Updates

None

2138	Firewatch				Report Issued	04/12/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
6	Low Priority	31/12/2019	-	Outstanding	1	Firewatch Integration Team

Control Issue

It was possible to access, complete and submit an Action Slip via the staff intranet which was not in adherence to proper practice.

Recommendation

If Action Slips do not need to be freely available to staff outside of HR, then access to this document should be restricted to appropriate personnel.

Action Details

HR to remove the Action Slip form from the intranet or restrict access to it to solely members of the HR team.

Status Updates

None

2138	Firewatch				Report Issued	04/12/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
7	Low Priority	31/01/2020	-	Outstanding	1	Firewatch Integration Team

Control Issue

Checks on large scale inputs to Firewatch in terms of uploads of leave entitlements were being undertaken, but these were not being evidenced.

Recommendation

The check undertaken by HR on the uploads of annual leave entitlements should be evidenced. This could be achieved by the officer completing the checks signing and dating the report from Firewatch. To add a further control, this could be undertaken by an independent officer with both officers involved recording their names and the date of the checks to evidence this.

Action Details

Reports are available which return details of Holiday Entitlements for personnel. Nicky will revisit these with HR to confirm they meet their requirements and if not, what amendments are required. HR to affirm the process amongst their team members.

Status Updates

None

2138	Firewatch				Report Issued	04/12/2019
Rec Number	Rating	Action Date	Revised Action Date	Status	Reminders Sent	Responsible Officer
8	Low Priority	31/01/2020	-	Outstanding	1	Firewatch Integration Team

Control Issue

Absence data was being manually transferred from Firewatch for manipulation within a spreadsheet by HR to track staff reaching trigger points defined by the Absence Management policy.

Recommendation

Investigations should take place to determine whether absence trigger points according to the Absence Management policy can be applied to the data in Firewatch to highlight to managers where their staff have reached these triggers and require a Return to Work interview. Managers could have this report added to their suite of reports in Firewatch.

Action Details

Reports identifying ‘trigger’ points have now been created negating the need for HR colleagues to extract and manipulate data outside of Firewatch. HR to test & confirm these.

Status Updates

None

Staffordshire
County Council