

ISLE OF ANGLESEY COUNTY COUNCIL	
Report to:	Audit and Governance Committee
Date:	23 July 2019
Subject:	Internal Audit Update
Head of Service:	Marc Jones Head of Function (Resources) / S151 Officer 01248 752601 MarcJones@ynysmon.gov.uk
Report Authors:	Marion Pryor Head of Audit and Risk 01248 752611 MarionPryor@ynysmon.gov.uk
Nature and Reason for Reporting: This report provides information on work carried out by Internal Audit since the last Committee meeting. It allows the Committee to monitor Internal Audit's performance and progress as well as providing summaries of Internal Audit reports so that the Committee can receive assurance on Council services and corporate areas.	

1. INTRODUCTION

1.1. The report provides an update as at 30 June 2019 on:

- Internal Audit reports issued since 16 April 2019
 - CONTEST – Countering Terrorism (separate report)
 - Welfare Reform – Housing Rent Income (separate report)
 - Schools Information Governance Health Check
- Follow up of internal audit reports
 - Payment Card Industry Data Security Standard Compliance
- Addressing 'Issues/Risks'
- Progress in delivering the Internal Audit Operational Plan 2019/20
- Standardisation of Assurance Ratings and Definitions
- CIPFA Statement on the Role of the Head of Internal Audit

2. RECOMMENDATION

2.1. That the Audit and Governance Committee notes Internal Audit's latest progress in terms of its service delivery, assurance provision, reviews completed, performance and effectiveness in driving improvement and decides whether it needs any further assurance on audit reports.



INTERNAL AUDIT UPDATE

JULY 2019

Marion Pryor BA MA CMIIA CPFA, Head of Audit & Risk

MarionPryor@YnysMon.gov.uk

01248 752611



TABLE OF CONTENTS

INTERNAL AUDIT REPORTS ISSUED	3
CONTEST - Countering Terrorism	3
Welfare Reform - Housing Rent Income	4
Schools Information Governance Health Check	4
FOLLOW UP OF INTERNAL AUDIT REPORTS	5
Payment Card Industry Data Security Standard Compliance	5
Follow Ups in Progress	6
Follow Ups Scheduled	6
ADDRESSING 'ISSUES/RISKS'	7
PROGRESS IN DELIVERING THE INTERNAL AUDIT OPERATIONAL PLAN 2019/20	8
STANDARDISATION OF ASSURANCE RATINGS AND DEFINITIONS	9
CIPFA STATEMENT ON THE ROLE OF THE HEAD OF INTERNAL AUDIT	10
APPENDIX A - INTERNAL AUDIT OPERATIONAL PLAN 2019/20	11

INTERNAL AUDIT REPORTS ISSUED

1. This section provides an overview of internal audit reports finalised since the last meeting, including the overall assurance rating and the number of issues/risks raised in the report's action plan. In accordance with the new audit approach, members of the committee and the relevant portfolio holder have received full copies of the report separately.
2. We have finalised **three** reports in the period, summarised below:

Title	Assurance Level	Critical	Major	Moderate	Total
CONTEST - Countering Terrorism	Reasonable	0	4	0	0
Welfare Reform - Housing Rent Income	Reasonable	0	1	3	4
Schools Information Governance Health Check	Not applicable	n/a	n/a	n/a	n/a

CONTEST – Countering Terrorism

Reasonable Assurance	Issues/Risks	
	0	Critical
	4	Major
	0	Moderate

3. Our review sought to answer the following key question:
Does the council have adequate arrangements in place to successfully discharge its statutory 'Prevent' duty under the Counter Terrorism and Security Act 2015, as outlined in HM Government's Counter Terrorism Strategy (CONTEST) 2018?
4. Overall, our review concluded that the council is making **good progress** in implementing an effective framework of controls to ensure that it can successfully discharge its statutory 'Prevent' responsibilities in respect of HM Government's Counter Terrorism Strategy (CONTEST) 2018.
5. We have raised four issues/risks that require management attention, which due to the potential impact of the risk in this area, are classed as 'Major' and are discussed in the report issued separately. However, the outcome of our review is mainly positive and therefore we are able to provide '**Reasonable**' assurance of the governance, risk management and control of this area. We have agreed an action plan with management, which we have detailed in a separate document.

Welfare Reform – Housing Rent Income

Reasonable Assurance	Issues/Risks	
	0	Critical
	1	Major
	3	Moderate

6. Our review sought to answer the following key question:

Does the council have adequate arrangements in place to manage the implications of welfare reform, specifically the impact on the council's ability to collect its housing rent income?

7. Overall, our review concludes that the council has a number of **effective operational controls** in place to manage the impact on the council's ability to collect its housing rent income.
8. While we have raised four issues/risks, which require management attention, the outcome of our review is mainly positive. We have agreed an action plan with management, which we have detailed in a separate document. Therefore, within the scope of our review, we are able to provide '**Reasonable**' assurance of the governance, risk management and control of this area.

Schools Information Governance Health Check

9. We commissioned the Strategic Risk Practice of Zurich Risk Engineering (ZRE) to conduct a health check of information governance and General Data Protection Regulation (GDPR) embedding across all the schools on the Island. This involved a situational questionnaire containing educational sector specific GDPR scenarios plus face-to-face interviews with six selected schools to understand their approaches to information governance and data protection. A member of the internal audit team accompanied the visits to schools and co-ordinated the issuing and collating of responses from the questionnaires. ZRE also reviewed the training material delivered as part of the Learning Service's GDPR programme.
10. As this was a consultancy piece of work and for internal information only, we have not provided an assurance rating. In addition, we will not be requiring the Head of Learning to formulate an action plan and we will not be formally tracking the recommendations made by the consultant. However, we will revisit this area as part of our routine follow up work, later in the year.
11. It is clear from the consultant's findings that schools have made progress with moving to compliance with GDPR but progress is being significantly hampered by the Learning Service's inability to recruit a Data Protection Officer (DPO). Despite externally advertising the post three times (twice in September 2018 and once in May 2019), the Learning Service has failed to recruit a suitable candidate. At the time of writing, the Learning Service has advertised the post internally, with a closing date of 05/07/19.
12. GDPR mandates the appointment of a DPO for all public bodies including all state-run schools because their core activities involve 'regular and systematic monitoring of data subjects on a large scale'. While the regulations do not specify any relevant qualifications that DPOs need it does require a DPO to have 'expert knowledge of data protection law and practices'. Not having a DPO in place increases the risk of non-compliance with data protection legislation and increases the potential for significant regulatory fines by the Information Commissioner's Office (ICO) should a significant data breach occur. There are also further risks of ICO investigation / enforcement in not appointing a dedicated DPO should a significant reportable incident occur and a risk of reputational damage for both schools and the council.

FOLLOW UP OF INTERNAL AUDIT REPORTS

13. Currently, we follow up all reports with an assurance rating of ‘Limited’ or below. We have finalised one follow up review in this period, with the following outcome. Further details of the work undertaken follow below:

Title of Audit	Review	Follow Up Concluded	Assurance Level	Critical	Major	Moderate	Total
Payment Card Industry Data Security Standard Compliance	Second Follow Up	June 2019	Reasonable	0	0	1	1

Payment Card Industry Data Security Standard Compliance

14. We undertook a review of compliance with the Payment Card Industry Data Security Standard (PCI DSS) compliance during 2016/17 with the final report issued in September 2016. This resulted in a ‘Limited Assurance’ rating, with 19 recommendations.
15. We conducted the first follow up review in December 2017 and found management had made little progress, with only two of the original recommendations implemented. Recommendations were amended and reiterated in the action plan, in accordance with the new audit approach of raising ‘issues’ and ‘risks’. This resulted in 11 ‘issues/risks’ outstanding after the first follow up.
16. We finalised our second follow up in June 2019, which concluded that **management have undertaken significant work** to address the issues/risks outstanding. We can confirm that the council now has a formal plan in place, which a project team reviews and monitors on a regular basis. There is a standing group to ensure continued compliance going forward. The council complies with PCI DSS and compliance certificates are available for each department. Policies and procedures have been developed and distributed to all applicable staff, and the project team has developed a training package. All staff involved with payments have reviewed and accepted the training package. It is mandatory for all staff involved with payments.
17. The council is now aware of the card payment environment, and the project manager has mapped the transaction types for each department. The project manager will develop this further as the council adds other departments.
18. The project team is capturing the existing set up of the PCI DSS components and will support the assessment of any impacts that changes to the IT infrastructure could have.
19. Our follow up review confirms that the council is now in a **strong position to demonstrate PCI DSS compliance** and there is a robust foundation in place to ensure continued compliance. Of the 11 risks / issues outstanding after the first follow up in January 2018, management have addressed 10 with one still in progress. We are therefore able to re-score our assurance rating and provide ‘Reasonable’ assurance in this area.

Follow Ups in Progress

20. We have **two** follow ups of reports with a ‘Limited Assurance’ rating currently in progress:

Title of Audit	Review	Date of Follow Up	Assurance Level	Critical	Major	Moderate	Total
Primary Schools – Income Collection	First Follow Up	Jun-19	Limited	0	2	1	3
Sundry Debtors	Second Follow Up	Jul-19	Limited	0	4	7	11

Follow Ups Scheduled

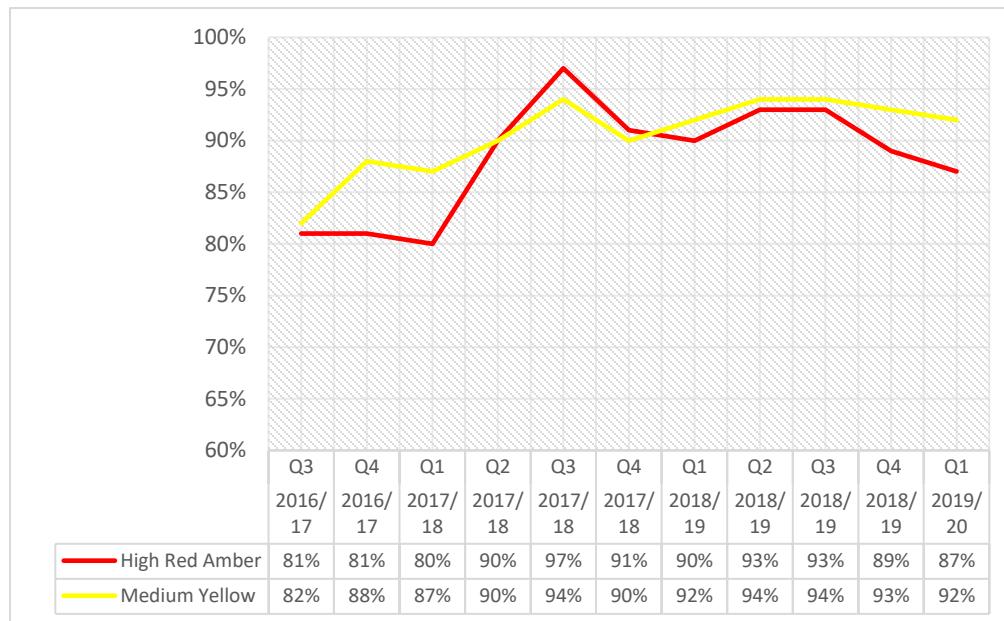
21. Currently, we have **three** follow ups scheduled for the remainder of the year. These may be added to dependent on the assurance provided for reviews we conduct throughout the year:

Title of Audit	Review	Date of Follow Up	Assurance Level	Critical	Major	Moderate	Total
Direct Payments	First Follow Up	Sep-19	Limited	0	0	5	5
System Controls – Logical Access and Segregation of Duties	Fourth Follow Up	Jul-19 October 2019 ¹	Limited	0	3	2	5
Schools Information Governance	First Review	November 2019	Not applicable	n/a	n/a	n/a	n/a

¹ The management actions to address the ‘Issues/Risks’ raised in the System Controls - Logical Access and Segregation of Duties review are dependent on the restructure of the Payroll/Payments function which is currently in progress, with an expectation that it will be complete by September 2019. Therefore, we have postponed the follow up review until it is complete.

ADDRESSING 'ISSUES/RISKS'

22. The graph below highlights management performance in addressing 'issues/risks' and implementing actions.



23. Although no High or Red issues/risks remain unaddressed, there has been a slight dip in addressing High/Red/Amber issues/risks, from 89% in quarter 4 of 2018/19 to 87% in quarter 1 of 2019/20. This is due to a small number of issues/risks becoming due at the end of June (which coincided with our reporting deadline) as a result of the recent Gypsies and Travellers and CONTEST (Counter Terrorism) audits. There are also several issues/risks, which are showing as outstanding on the system relating to the 'Primary Schools - Income Collection' audit, which we are currently following up.
24. The slight dip in performance for the Medium/Yellow risks from 93% to 92% is due in the main to the 'Leisure Services - Governance and Control' audit where similarly, several yellow issues/risks came due at the end of June.
25. We have had notice from our software providers that the new and upgraded version of the action tracking system is now available, which provides extra functionality and reduces the burden of administering the system.
26. Following implementation of the new software upgrade, we will undertake an exercise to cleanse the historical data and review the system configuration. We will also take the opportunity to review our reporting framework to ensure that the information provided to senior management and the Audit and Governance Committee is in line with the new audit approach and is concise, relevant and timely. In anticipation of the upgrade, we have switched off the automatic email reminders and this may account for managers not updating the system.
27. The IT team are currently progressing with the implementation, although this has been delayed due to a bereavement in the team.

PROGRESS IN DELIVERING THE INTERNAL AUDIT OPERATIONAL PLAN 2019/20

28. The Operational Plan for 2019/20 is at [Appendix A](#).
29. We were hoping to finalise and report the outcome of **four** audits to the committee at this meeting but for a variety of reasons, this has not been possible:
 - **Business Continuity Arrangements** - although it was started, due to long-term sickness absence, this audit has had to be postponed until another member of the team is free to continue with it
 - **Corporate Safeguarding Follow Up** - in response to concerns raised by the Monitoring Officer, we have increased the scope of this audit significantly, which is inevitably taking longer to complete
 - **IT Resilience** - in response to a request from the Head of IT, a short delay in the audit is necessary as the council is currently undergoing a mandatory Cyber Essentials+ accreditation process, which is invasive to the network and systems, and resource intensive. Consequently, the Head of IT cannot accommodate both pieces of work and the Cyber Essentials+ must take priority. In addition, the IT team is undertaking a resilience test using its disaster recovery plan and a specific scenario to test the failure of an entire datacentre, to review how effectively the documentation and processes operate in relation to bringing systems online at the alternative datacentre. The outcome will inform the resilience audit.
 - **Corporate Information Governance Health Check** - following our experience of using an external assurance provider to review schools, in consultation with the Corporate Information Governance Manager, it was felt that we could undertake this piece of work more effectively internally. However, due to long-term sickness absence, we have not been able to progress with this piece of work.
30. In addition to the two follow up audits detailed earlier, work continues on the Corporate Safeguarding audit, along with a review of Welfare Reform and the impact on our obligations around homelessness, along with scoping a review of the council's financial resilience.
31. Following the recommendation in the Corporate Risk Management Health Check for the corporate risk register to be reviewed and the corporate risks to be rationalised, the Senior Leadership Team has reviewed the corporate risk register and reduced the corporate risks by around a half. This is reflected in the internal audit priorities going forwards.

STANDARDISATION OF ASSURANCE RATINGS AND DEFINITIONS

32. Standard 2410 of the Public Sector Internal Audit Standards requires the ‘final communication of engagement results’ (audit reports) to include applicable conclusions. Where appropriate, internal auditors should provide an opinion, which may be ratings, conclusions or other descriptions of the results. The formulation of the opinion requires consideration of the results and their significance.
33. In line with the above and as part of the continuous improvement of our audit approach, we reviewed the definitions of our assurance ratings, submitting them to this committee for comment at its meeting in April 2019.
34. The committee sought clarification of whether there is a standard national definition of assurance ratings. In addition, if there was not, whether in the interests of benchmarking and consistency, we should introduce standard definitions.
35. We confirmed that a standard definition for assurance ratings was not in use. To determine the support for standardised assurance ratings and definitions, a query was sent to all the heads of audit across Wales and to the Governance Advisor at CIPFA’s Better Governance Forum, for their comments.
36. The exercise confirmed that the councils’ definitions are not dissimilar, with the following being generic terms common to most councils:
 - substantial or high
 - reasonable or adequate
 - limited or minimal
 - no assurance.
37. However, of the 14 responses, only one supported the idea of standardised assurance ratings and definitions. The majority cited the advantage of local flexibility, which allows auditors to report and present conclusions in a way most suited for their organisation, in line with the organisation’s own risk appetite. Standard definitions could only be used at a very high level due to the varying scopes of the audits and audit approach. In addition, since the Public Sector Internal Audit Standards (PSIAS) does not even mandate a rating be given, the use of a standard system could not be enforced.
38. The CIPFA Benchmarking Group has also explored this area. The CIPFA Governance Adviser confirmed that although CIPFA does not mandate standard definitions, there has always been some sharing of practice.

CIPFA STATEMENT ON THE ROLE OF THE HEAD OF INTERNAL AUDIT

39. CIPFA launched its Statement on the Role of the Head of Internal Audit in April 2019. It called on the public sector to provide recognition, support and encouragement for heads of internal audit and their teams.
40. ‘The role of the head of internal audit’ sets out five principles, aligned with the UK Public Sector Internal Audit Standards (PSIAS), that outline the key expectations of heads of internal audit and the conditions that will allow them to thrive.
41. The principles set out individual and organisational responsibilities, and represent best practice guidance that can form the basis of conversations between internal auditors, leadership teams and audit committees to support internal audit effectiveness.
42. On launching the statement, the CEO of CIPFA commented, “heads of internal audit across the whole public sector are working in increasingly high pressure environments, contending with restricted resources and growing levels of financial risk. While many organisations are already doing a great job in this space, it is crucial that heads of internal audit and their teams are given the tools they need to provide quality assurance to their organisations.”
43. CIPFA also launched a collection of case studies to accompany the refreshed statement. ‘Leading internal audit in the public sector: putting principles into practice’ gives a series of examples of organisations across the public sector that are leading the way with innovative solutions to provide better support and assurance to their organisations and clients.
44. The documents can be downloaded at:

<https://www.cipfa.org/roleofthehia>

<https://www.cipfa.org/leadinginternalaudit>

APPENDIX A – INTERNAL AUDIT OPERATIONAL PLAN 2019/20

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
CORPORATE-WIDE								
Corporate	Business Continuity (YM9)	Corporate Risk Register	C2	C2	10	0.5	Work in progress – temporarily postponed	
Corporate	Welfare Reform – Universal Credit and Housing Rent Income (YM 10)	Corporate Risk Register	B2	C2	0	7.75	April 2019 (2018/19)	
	Welfare Reform – Homelessness (YM10)				10	3.25	Work in progress	
Corporate	Corporate Safeguarding (YM11)	Corporate Risk Register	C2	D2	15	10	December 2018 (2018/19)	
	CONTEST (Countering Terrorism and Preventing Radicalisation) ² (YM11)	Corporate Risk Register			0	0	Work in progress	
							April 2019 (2018/19)	

² Previously a 'stand-alone' risk - YM27

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
Corporate	Corporate Planning (YM13)	Corporate Risk Register	D2	D3	10	0		
Corporate	Financial Resilience (YM41)	Corporate Risk Register	A1	B2	15	0	Scoping in progress	
Corporate	Information Governance (YM3)	Corporate Risk Register	B3	C3	0	0	December 2018 ³ (2018/19)	
Corporate	Payment Card Industry Data Security Standards (PCIDSS) (YM34)	Corporate Risk Register	D1	D1	7	7	June 2019	
Corporate	Brexit	Corporate Risk Register	A2		5	0		
Corporate	Leavers' Process	Concerns raised			10	0		
Corporate	Risk Management	PSIAS requirement			5	0	February 2019 (ZRE)	
Corporate	Managing the Risk of Fraud	PSIAS requirement			20	0		
Corporate	Culture – Protecting Reputation and the Use of Social Media	Horizon Scanning			10	0		
Corporate	Well-being of Future Generations Act	High-profile legislation			0	0	Incorporated within each audit	

³ Assurance provided for General Data Protection Regulations previously 'stand-alone' Amber Risk (YM31)

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
Corporate	Social Services and Well-being Act – Part 9 Requirements	High profile legislation			0	0	Implementation postponed	
RESOURCES								
Resources	Recovery and Write-offs	Key Financial System - S151 concerns			10	0		
Resources	Corporate Procurement (YM22)	Corporate Risk Register	B2	D2	10	0	December 2018 (2018/19)	
Resources	Corporate Procurement Cards	Concerns raised			20	0		
Resources	Payroll	Key Financial System - restructure and new system; external audit assurance			20	0		
COUNCIL BUSINESS								
Legal Services	Land Registration (YM26)	Corporate Risk Register	C1	E2	0	0	Risk now closed	
TRANSFORMATION								
ICT	IT Audit - Cyber Security (YM28)	Corporate Risk Register	B1	C1	15	0	February 2019 (2018/19)	
ICT	IT Audit - IT Resilience (YM38)	Corporate Risk Register	C1	D2	15	2	Work in progress	

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
Human Resources	Sickness Absence (YM23)	Corporate Risk Register	A2	D3	10	0		
Human Resources	Recruitment & Retention (YM5)	Corporate Risk Register	B2	C2	10	0	April 2019 (2018/19)	
Human Resources	Workplace Culture – Discrimination and Staff Inequality	Horizon Scanning			10	0		
REGULATION & ECONOMIC DEVELOPMENT								
Regulation & Economic Development	Infrastructure projects (YM17)	Corporate Risk Register	B2	D2	20	0.25		
Regulation & Economic Development	Leisure Services - Investment in Facilities (YM32)	Corporate Risk Register	B2	B3	10	0		
Regulation & Economic Development	Leisure Services - Governance and Control	Head of Service Request - major structural changes (carried forward from 2018/19)			2	2	April 2019 (2018/19)	
HIGHWAYS, WASTE & PROPERTY SERVICES								
Property	Asset Management	Horizon scanning			10	0		

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
Highways	Bridges	Horizon scanning			0	0		
HOUSING								
Housing	Gypsies and Travellers (Requirements of the Housing Act 2014) (YM29)	Corporate Risk Register	B2	C2	0	0	April 2019 (2018/19)	
ADULT SERVICES								
Adults	Deprivation of Liberty Safeguards (YM25)	Corporate Risk Register	C2	D3	0	0	Risk now closed	
Adults	Continuous Healthcare	Horizon scanning	n/a	n/a	10	0		
CHILDREN'S SERVICES								
Children's	Integrated Service Delivery Board (YM36)	Corporate Risk Register	B2	C2	0	0	Risk now closed	
Children's	Social Work Practice (YM37)	Corporate Risk Register	C2	D2	0	0	Risk now closed	
LEARNING								
Learning	Schools Modernisation (YM15)	Corporate Risk Register	C2	C2	20	0		
TOTAL AUDIT DAYS					314⁴	32.75		

⁴ Previously 420 days

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
CHARGEABLE NON PROGRAMMED DAYS (PRODUCTIVE)								
	Follow Up Work	Several limited assurance reports requiring follow up, includes reporting and administering 4Action			60	14		
	General Counter Fraud Work, National Fraud Initiative (NFI)				30	1.25		
	Referrals				40	2.75		
	Closure of Previous Year's Work				13	13		
	Grant Certification:	Grant Requirement			20			
	School Uniform Grant					0		
	Rent Smart Wales Grant					0		
	Education Improvement Grant					0		
	Pupil Development Grant					0		
	Sixth Form & Adult Continuing Learning					0		
	Corporate consultancy					50	18.75	

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
	Audit & Governance Committee, including training for members and self-assessment				60	10.5		
	Management Review				50	6.75		
	Contingency				0	0		
	TOTAL				323⁵	67		
NON CHARGEABLE DAYS (NON-PRODUCTIVE)								
	Risk & Insurance				24	5.5		
	General Administration				40	11.5		
	Personal Development & Review, 121 & Team Meetings				35	3		
	Management, including liaison with External Audit and audit plan preparation				50	11.75		
	Leave, including annual, statutory, special and sick leave				414 ⁶	164.25		
	Training and Development for staff				100	29.5		
	TOTAL				663⁷	226		

⁵ Previously 440 days

⁶ Previously 182 days

⁷ Previously 440 days

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Inherent)	Corporate Risk Rating (Residual)	Revised Indicative Days 2019-20	Actual Days as at 30/06/19	Notes / Assurance Rating / Date Last Undertaken	Target / Actual Date of Reporting to Committee
	TOTAL RESOURCE REQUIREMENT				1300			
	RESOURCE AVAILABLE				1300	325		
	RESOURCE SHORTFALL				0	0		
	PRODUCTIVITY				50%⁸	31%		

⁸ Previously 67%