ISLE OF ANGLESEY COUNTY COUNCIL	
Report to:	Audit and Governance Committee
Date:	12 February 2019
Subject:	Internal Audit Update
Head of Service:	Marc Jones, Head of Function (Resources) / S151 Officer 01248 752601 MarcJones@ynysmon.gov.uk
Report Author:	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 27 January 2019 on:

- Internal Audit reports issued since 10 November 2018
- Follow up of internal audit reports
- Implementation of management actions
- Progress in delivering the Internal Audit Operational Plan 2018/19
- Risk Management Health Check

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.

CYNGOR SIR
YNYS MÔN
ISLE OF ANGLESEY
COUNTY COUNCIL

Internal Audit Update

February 2019

Marion Pryor BA MA CMIIA CPFA
Head of Audit & Risk

Contents

Internal Audit reports recently 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.

2. We have finalised **one** report in the period, summarised below:

Title	Assurance Level	Catastrophic	Major	Moderate	Total
IT Cyber Security	**Reasonable**	0	2	3	5

IT Cyber Security[1]

	Issues/Risks	
Reasonable Assurance	**0**	**Catastrophic**
	2	**Major**
	3	**Moderate**

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

   Does the Council have adequate protection, detection and response arrangements in place to mitigate the risk to the Council's network, systems, information and services from a cybersecurity breach?

4. Overall, our review concluded that the Council has a number of effective, operational controls in place to manage the risk to cybersecurity and to prevent and reduce the impact to Council services, systems and information of malicious, external attacks.

5. However, a lack of proactive monitoring of the extent and nature of current and emerging cyber threats faced by the Council could compromise success in this area. In addition, scrutiny and reporting arrangements, particularly at Head of Service level, need to be strengthened. As senior management are best placed to provide resources and influence staff behaviour with regards computer use and cyber safety, effective engagement at this level is imperative.

6. The Council has comprehensive IT policies in place that cover cybersecurity risks, and at the time of our review 92% of staff with computer access had read and accepted the Information Security Policy. We did however identify a small number of

[1] As part of a new report style pilot, members of the Audit and Governance Committee and the relevant Portfolio Holder have received a copy of the full report ahead of this meeting.

inconsistencies between this and the Council's Digital Strategy regarding 'Bring Your Own Device (BYOD) which need to be resolved.

7. The Council has recently reviewed and strengthened its corporate password requirements in line with nationally recommended criteria. However, the password complexity settings for two of the Council's externally facing systems do not adhere to this, and are insufficient to adequately protect against a data breach.

8. Protection of the Council's network is clearly a priority for IT and a variety of technical safeguards are in place in order to achieve this. Despite this discernible success, our review found that controls around removable media devices do not reflect the requirements in this area as outlined in the IT Security Policy. A review to ensure only those authorised to use removable media devices are able to do so would reduce the risk of security or data breaches.

9. While we raised five issues/risks, which require management attention, the outcome of our review is mainly positive. We have agreed an action plan with management, which is detailed in a separate document. Therefore, within the scope of our review, we are able to provide a **reasonable level of assurance** in this area.

Follow up of Internal Audit reports

10. 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:

Title of Audit	Review	Assurance Level	Catastrophic	Major	Moderate	Minor	Total
Logical Access and Segregation of Duties	Third Follow Up	**Limited**	0	2	1	0	3

Logical Access and Segregation of Duties – Third Follow Up

11. *In accordance with the Audit and Governance Committee's resolution with regards 'Limited Assurance' reports, I have provided a copy of the full report to the members separately.*

12. We undertook a review of logical access and segregation of duties controls as part of the annual Internal Audit Plan in 2014/15. This resulted in a 'Red' rating, defined at the time as *'Taking account of the issues identified, the Council cannot take assurance that the controls upon which the organisation relies to manage these risks are suitably designed, consistently applied or effective. Action needs to be taken to ensure these risks are managed.'*

13. The review resulted in 15 recommendations and one suggestion being made.

14. We undertook a follow up review in January 2015, which again resulted in a 'Red' rating. Twelve recommendations remained outstanding and the 'Red' rating remained.

15. A second follow up review took place in December 2017, which confirmed that five remained unaddressed. Consequently, this review resulted in a 'Limited Assurance' rating (in accordance with the new audit approach).

16. In December 2018, we undertook a third follow up review. This confirmed that from the five issues / risks outstanding, two have been addressed and three are in the process of being addressed.

17. The payroll section is currently in the process of undergoing a restructure. Once the Northgate project is finished, the new structure will be implemented. The first round of consultations on the new structure has just taken place and this will progress during January 2019. Once implemented, the Accountancy Service Manager is confident that this will address the remaining issues/risks originally raised.

18. Taking consideration of the results of our follow up review, although progress has been made, the assurance level of the report remains as a **'Limited Assurance'** at this time and we will undertake a further follow up during July 2019.

Follow Ups Scheduled and In Progress

19. We have **two** reports with a 'Limited Assurance' rating scheduled for a follow up review before the end of this financial year. Both follow-up reviews are currently in progress:

Title of Audit	Reason for Review	Date of Follow Up	Assurance Level	Catastrophic	Major	Moderate	Minor	Total
Child Care Court Orders Under the Public Law Outline	Second Follow Up	Jul-18 (Draft Report issued)	**Limited**	1	3	3	1	8
Payment Card Industry Data Security Standard Compliance	Second Follow Up	Oct-18 (postponed until Feb-19 at the request of the Head of Resources due to change in project milestones)	**Limited**	0	6	4	1	11

Implementation of Management Actions

20. A detailed report of all outstanding Red and Amber Issues/Risks is made separately.

21. A recent exercise to examine the historical data included in the action tracking system has highlighted an overly administrative configuration and items inconsistent with our risk-based approach to auditing. A new and upgraded version of the action tracking system will shortly be available, which provides extra functionality and reduces the administrative burden. Therefore, we will undertake an exercise next year to cleanse the historical data and review the system configuration.

Progress in delivering the Internal Audit Operational Plan 2018/19

22. The current Plan is attached at Appendix A. Since the appointment of the two new Senior Auditors, work has progressed well. However, going forward, along with the length of these vacancies, protracted investigations, significant follow up work and the maternity leave of the third Senior Auditor, which started unexpectedly in October 2018, our target for undertaking 80% of the red and amber residual risks in the corporate risk register will be difficult to achieve.

23. Although we have only covered **35%** of the red and amber residual risks in the corporate risk register, work is currently ongoing in **five** areas which are included as red and amber residual risks in the corporate risk register:

    - Gypsies and Travellers (Requirements of the Housing (Wales) Act 2014)
    - Counter Terrorism and the 'Prevent' Duty
    - Recruitment and Retention
    - Business Continuity (two red risks)
    - Welfare Reform

24. Work is also ongoing in **three** areas at the request of Heads of Service, which are not included in the corporate risk register:

    - Direct Payments
    - Leisure Services – Governance Arrangements
    - Car Loans – Recovery Arrangements

25. We are also involved in two ongoing investigations, which are both nearing their conclusion.

Risk Management Health Check

26. We underwent an independent Risk Management Health Check by our insurers, Zurich Municipal (ZM). In order to measure the maturity of risk management, ZM used a Performance Model which breaks down risk management activity into six categories that contribute towards effective risk management arrangements within an organisation:

    - Risk culture and leadership
    - Risk appetite and strategy
    - Governance
    - Methodology
    - People and training
    - Projects, partnerships and supply chain

27. The model enabled ZM to make an assessment about the extent to which risk management is having a positive effect on the organisation. ZM concluded that risk management was at a **'Managed'** level within the five levels of maturity as follows:

Level 1 Fragmented	Level 2 In Development	Level 3 Managed	Level 4 Integrated	Level 5 Transformational

28. ZM commented that:

29. *"Since 2015, a new senior team has been established at IoACC, previously in special measures the council are now moving forward in embedding risk management. There is clear evidence that the organisation recognises the need to encourage and engage in wider cross-service risk management.*

30. *The current number of strategic risks on the risk register seems disproportionate to other similarly sized Local Authorities (circa 37 risks). Usually between 10 to 15 risks are managed at a Corporate / Strategic Level. The recent move to a new 4risk system,*

whilst a positive step, will not facilitate a change in the current risk culture and risk maturity at IoACC. There are isolated pockets of services fully engaging with the Risk and Insurance Manager and routinely updating 4risk as per requirements. The interviews revealed that the risk management process, for a variety of reasons, has not fully embedded across the Council.

31. *There appears to be a fragmented approach to formal project risk recording; a form of PRINCE 2 is currently in use across IoACC however, a standard RAID[2] template is not being adopted or completed across the council's current project portfolio. When requested during the interview process it was stated that project risks are considered in theory at project outset. No formal evidence or documentation was supplied to validate that claim. The findings of the recent IoACC Internal Audit in which the approach to project management was deemed "Reasonable Assurance" raised issues / risks which further supports the view. It is recommended that Risk Management consider the role they can play in supporting successful project delivery across IoACC and throughout the project life-cycle.*

32. *Although some of the baseline assessment areas may appear low, there is evidence that improvements are relatively easy to implement. Higher maturity levels could easily be attained if the strategic risks are reviewed and agreed to more manageable levels. The lack of updating of risks, controls and mitigating actions using the 4risk and 4action modules is also a major concern in providing assurance that risks are being managed and co-ordinated effectively across all services.*

33. *There are a number of priority areas for improvement:*

    - *Refresh the Strategic and Service / Directorate risk registers in light of introduction of 4risk with an emphasis on identifying only the key risks affecting IoACC.*
    - *Consider a Strategic level BREXIT Risk – given the prominence of the Port at Holyhead and Wylfa Power Station proposals / potential long-term fiscal impacts.*
    - *Review how risks within projects (and partnerships) are included within the Corporate Risk Management arrangements. Visibility, prominence and risk management team representation.*
    - *Ensure Project Risk and Prince 2 documentation and risk identification are aligned to ensure successful project delivery.*
    - *Identify nominated Risk Champions within each service to support and embed consistent application and usage of 4risk."*

34. The outcome was largely as expected and we are currently developing an Action Plan to address all the observations / recommendations raised by ZM.

---

[2] [The acronym RAID stands for Risks, Assumptions, Issues and Dependencies.]

Appendix A – Internal Audit Operational Plan 2018/19[3]

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Residual)	Revised Plan 2018/19	Actual Days as at 27/01/19	Notes / Assurance Rating	Target / Actual Date of Reporting to Committee
CORPORATE-WIDE							
Corporate	Business Continuity	Corporate Risk Register	C2 - YM9 C1 - YM38	10	2		April 2019
Corporate	Welfare Reform	Corporate Risk Register	C2 YM10	10	1.5		April 2019
Corporate	Corporate Safeguarding	Corporate Risk Register	D2[4] YM11	7	7	**Reasonable Assurance**	**December 2018**
Corporate	CONTEST (Countering Terrorism and Preventing Radicalisation)	Corporate Risk Register	E1 YM27	10	3.5		April 2019
Corporate	Payment Card Industry Data Security Standards (PCIDSS)	Corporate Risk Register	D1 YM34	15	7.75		April 2019
Corporate	General Data Protection Regulations (GDPR)	Corporate Risk Register	C2 YM31	8	8	**Reasonable Assurance**	**December 2018**
Corporate	Corporate Procurement	Corporate Risk Register	D2 - YM20 D2 - YM22	18	18	**Reasonable Assurance**	**December 2018**

[3] Corporate Risk Register approved by SLT 10/09/18
[4] Residual Risk reduced from C1 (Red) to D2 (Amber)

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Residual)	Revised Plan 2018/19	Actual Days as at 27/01/19	Notes / Assurance Rating	Target / Actual Date of Reporting to Committee
Corporate	Risk Management	New process implemented October 2017. New 4Risk software rolled out September 2018.	n/a	n/a	n/a	**Level 3 'Managed'[5]**	**February 2019**
Corporate	Well-being of Future Generations Act	High-profile legislation that has a significant impact on the way the Council works. It is subject to specific review by WAO.	n/a	0	0	Rolled forward to 2019/20	
Corporate	Social Services and Well-being Act - Part 9 requirements	High-profile legislation that has a significant impact on the way the Council works. Extension from WG to implement pooled budgets	n/a	0	0	Subject to consultation – rolled forward to 2019/20	
Corporate	Managing the Risk of Fraud	PSIAS requirement	n/a	0	0	Rolled forward to 2019/20	
RESOURCES							
Resources	Recovery and Write-offs (Car Loans)	Key Financial System - S151 concerns	n/a	10	3.5		April 2019
Resources	Income – Sundry Debtors Follow Up	Key Financial System - external audit assurance	n/a	18	18	**Limited Assurance**	**December 2018**

[5] Conclusion of an independent Health Check, conducted by Zurich Municipal based on their maturity model, which incorporates five levels of maturity

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Residual)	Revised Plan 2018/19	Actual Days as at 27/01/19	Notes / Assurance Rating	Target / Actual Date of Reporting to Committee
Resources	Payroll	Key Financial System - external audit assurance	n/a	0	0	Subject to ongoing changes – rolled forward to 2019/20	
TRANSFORMATION							
ICT	IT Audit - Cyber Security	Corporate Risk Register	C1 YM28	20	20	**Reasonable Assurance**	**February 2019**
HR	Recruitment & Retention	Corporate Risk Register	C2 YM5	15	8		April 2019
REGULATION & ECONOMIC DEVELOPMENT							
Regulation & Economic Development	Energy Island Programme	Corporate Risk Register	C2 - YM13 C2 - YM16 D2 - YM17	0	0	Rolled forward to 2019/20	
Regulation & Economic Development	Leisure Services – financial investment	Corporate Risk Register	B3 YM32	0	0	Rolled forward to 2019/20	
Regulation & Economic Development	Leisure Services - Governance and Control	Head of Service Request - major structural changes. Carried forward from 2017/18	n/a	15	4.75		April 2019
HIGHWAYS, WASTE & PROPERTY SERVICES							
Highways	Car Park Services – Enforcement	New pilot in place from 2017/18 with external organisation for car parking enforcement	n/a	0	0	Deleted – low priority	
Highways	Highways Contract Monitoring Arrangements	Head of Service request	n/a	10	10	**Substantial Assurance**	**September 2018**

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Residual)	Revised Plan 2018/19	Actual Days as at 27/01/19	Notes / Assurance Rating	Target / Actual Date of Reporting to Committee
HOUSING							
Housing	Gypsies and Travellers (Requirements of the Housing Act 2014)	Corporate Risk Register	C2 YM29	10	6.75		April 2019
ADULT SERVICES							
Adults	Deprivation of Liberty Safeguards	Corporate Risk Register	C2 YM25	9	9	**Reasonable Assurance**	**July 2018**
Adults	Direct Payments	Head of Service request (carried forward from 2017/18)	n/a	20	18.75		~~September 2018~~ April 2019
CHILDREN'S SERVICES							
Children's	Integrated Service Delivery Board	Corporate Risk Register	C2 YM36	0	0	Rolled Forward to 2019/20	
LEARNING							
Learning	General Data Protection Regulations (GDPR) - Implementation within Schools	Corporate Risk Register. Will be the subject of an independent Health Check by our insurers.	C2 YM38	n/a	n/a		April 2019
Learning	Primary Schools Thematic Reviews - Schools Income Collection	Head of Service request	n/a	20	20	**Limited Assurance**	**~~September 2018~~ December 2018**
GRANT CERTIFICATION							
	Rent Smart Wales Grant	Grant requirement	n/a	10	10	**Substantial Assurance**	**July 2018**
	School Uniform Grant					**Reasonable Assurance**	**September 2018**

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Residual)	Revised Plan 2018/19	Actual Days as at 27/01/19	Notes / Assurance Rating	Target / Actual Date of Reporting to Committee
	Education Improvement Grant					**Substantial Assurance**	**September 2018**
	Pupil Development Grant					**Substantial Assurance**	**September 2018**
	TOTAL AUDIT DAYS			**235**	**175.75**		
CHARGEABLE NON PROGRAMMED DAYS (PRODUCTIVE)							
	Follow Up Work	Several limited assurance reports requiring follow up, includes reporting and administering 4Action		70	65.75		
	National Fraud Initiative			10	8.5		
	General Counter Fraud Work, enquiries and referrals			50	42.25		
	Closure of Previous Year's Work			19	19		
	Corporate consultancy			55	50.5		
	Audit & Governance Committee, including training for members			40	35.25		
	Management Review			25	18.5		
	TOTAL			**269**	**239.25**		
NON CHARGEABLE DAYS (NON-PRODUCTIVE							
	Risk & Insurance			20	16.75		
	General Administration			40	32		

Service / Section	Title	Reason for Inclusion	Corporate Risk Rating (Residual)	Revised Plan 2018/19	Actual Days as at 27/01/19	Notes / Assurance Rating	Target / Actual Date of Reporting to Committee
	Personal Development & Review, 121 & Team Meetings			20	9.25		
	Management, including liaison with External Audit and audit plan preparation			40	31		
	Leave, including annual, statutory, special and sick leave			362	285.75		
	Training and Development for staff, including induction and Welsh lessons			111	84.25		
	TOTAL			**593**	**459**		
	TOTAL RESOURCE REQUIREMENT			**1096**			
	RESOURCE AVAILABLE			**1096**			
	RESOURCE SHORTFALL			**0**			