Agenda Item	**4**
Report No	**AS/2/22**

THE HIGHLAND COUNCIL

Committee: **Audit & Scrutiny Committee**

Date: **16th February 2022**

Report Title: **Internal Audit Reviews and Progress Report – 06/11/21 – 28/01/22**

Report By: **Corporate Audit Manager**

1. Purpose/Executive Summary

1.1 This report provides details of the work undertaken by the Internal Audit section since the last report to Committee in November 2021.

2. Recommendations

2.1 Members are asked to note the current work of the Internal Audit Section outlined at section 5 of the report and progress against the 2021/22 audit plan in section 6.

3. Implications

3.1 Risk – the risks and any associated system or control weaknesses identified as a result of audit work or corporate fraud investigations will be reviewed and recommendations made for improvement.

3.2 There are no Legal, Resources Community (Equality, Poverty, Rural and Island), Climate Change / Carbon Clever or Gaelic implications.

4. Audit Reports

4.1 There have been **2** final reports issued during this period as detailed in the table below:

Service Directorate	Subject	Opinion
Performance & Governance	Governance of Arms Length External Organisations and Partnerships (ALEOs)	Substantial Assurance
Transformation	Cyber Security	Reasonable Assurance

Each report contains an audit opinion based upon the work performed in respect of the subject under review. The five audit opinions are set out as follows:

(i) **Full Assurance**: There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.
(ii) **Substantial Assurance**: While there is a generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
(iii) **Reasonable Assurance:** Whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk**.**
(iv) **Limited Assurance**: Weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk.
(v) **No Assurance:** Control is generally weak, leaving the system open to significant error or abuse, and/ or significant non-compliance with basic controls leaves the system open to error or abuse.

5. Other Work

5.1 The Section has been involved in a variety of other work which is summarised below:

(i) Audits for other Boards, Committees or Organisations

Audit work has been undertaken for High Life Highland during this period and the results will be reported to their Finance and Audit Committee.

(ii) Corporate Fraud and other investigations activity

The Single Point of Contact (SPOC) work is an ongoing commitment providing information to Police Scotland and the Department of Work and Pensions.

With regard to the previous 3 investigations reported to Committee; 2 into missing money and 1 for personal misuse of a Council asset for personal gain, the fraud investigation work has been completed and reports provided to management. 1 of these is being reported to the Procurator Fiscal and an internal disciplinary investigation is being considered for another matter. For the final investigation, a system weaknesses report is being prepared and it is expected that this will be provided to the June Committee meeting for scrutiny.

During this period there have been 2 new cases referred to the section consisting of 1 fraud concern where the line manager prevented an employee claiming a payment to which they were not entitled. This prompt action stopped the potential

payment but this matter will be investigated further to establish whether this was an isolated incident or if this is indicative of culture and practice. In addition, a new whistleblowing concern is being assessed for investigation.

Work also continues into the investigation into 2 whistleblowing concerns and it is expected that the results of these will also be reported in June. The annual report on whistleblowing will also be presented to this meeting which will provide details of the overall number of whistleblowing concerns received, the outcomes and whether any areas for improvement were identified. As always, no further information can be provided for ongoing on-going fraud and whistleblowing investigations, but the necessary Committee scrutiny can be undertaken once fuller reports are provided at the appropriate time.

6. Progress against the 2021/22 audit plan

6.1 Progress against the audit plan is shown in the Gantt chart. This contains details are provided of all planned audits and any additions resulting from unplanned audits or investigations. In respect of investigations this information is added at the point that the system weaknesses draft report is issued as investigations may be complex and can be time consuming to complete.

The chart shows the dates that the key stages of each audit was completed except where the audit has rolled forward from last year and they occurred before 04/04/21, however, any stages after this date are shown.

6.2 The Trainee Auditor started in post on 01/02/22, slightly later than planned but this now means that the section has a full establishment of staff. This slippage has been accounted for by reducing the contingency time so there is no effect on the audit plan.

6.3 Performance information for quarter 3 is provided below.

Category	Performance Indicator	Target	2021/21 Actuals			
			Qtr 1	Qtr 2	Qtr 3	Qtr 4
Quality						
Client Feedback	(i) % satisfaction from individual audit engagements expressed through Client Audit Questionnaires (CAQ)	**75**	0	91	86	n/a
	(ii) % of Client Audit Questionnaires returned	**70**	0	100	100	n/a
Business Processes						
Timeliness of Final Report	(i) % of draft reports responded to by client within 20 days of issue	**85**	0	75	75	n/a
	(ii) % of final reports issued within 10 days of receipt of management response	**90**	0	100	100	n/a

Designation: Corporate Audit Manager

Date: 1st February 2022

Author: Donna Sutherland

AGENDA ITEM 4.1

Internal Audit Final Report

Performance and Governance

Governance of Arms Length External Organisations and Partnerships (ALEOs)

Description	Priority	No.
Major issues that managers need to address as a matter of urgency.	High	0
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	3
Minor issues that are not critical but managers should address.	Low	0

Distribution:

Executive Chief Officer for Performance and Governance
Executive Chief Officer for Education and Learning
Executive Chief Officer for Infrastructure, Environment and Economy
Head of Corporate Governance, Performance and Governance
Head of Resources, Education and Learning
Head of Roads and Transport, Infrastructure Environment and Economy
Corporate Audit and Performance Manager, Performance and Governance

Audit Opinion

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Substantial Assurance** can be given in that while there is generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Report Ref: HPG06/001
Draft Date: 10/11/21
Final Date: 16/12/21

1. Introduction

1.1 The audit assessed the Council's arrangements for governing its significant Arms Length External Organisations and Partnerships (ALEOs). The objectives of the review were to ensure that the Council has effective arrangements: to record its ALEOs and to train, support and guide members and officers; to identify, create and oversee its ALEOs; and to monitor its ALEOs to confirm they remain fit for purpose.

1.2 The scope of the review included testing to ensure that ALEOs are governed in accordance with the Council's own guidance and the good practice advice referred to in various Audit Scotland reports. The audit review considered the following significant ALEOs; High Life Highland (HLH); Eden Court; and Highlands and Islands Transport Partnership (HiTrans). The audit covered the period from April 2020 to October 2021.

Name	Year Created	Budgeted Funding £000s	
		2020/21	2021/22
Eden Court	1977	300	300
HiTrans	2005	91	91
High Life Highland	2011	16,170	16,816

2. Main Findings

2.1 *Recording of ALEOs*

The audit objective was substantially achieved. Financial Regulation 26.3.2 requires that "A register of Arm's Length Organisations who receive funding from the Council will be maintained by the Chief Financial Officer" and that the register should record specific key information. The Head of Corporate Governance (rather than the Chief Financial Officer), as company secretary holds and maintains key records for each ALEO, however this is not fully compliant with Financial Regulation 26.3.2. (See Action Plan Reference: M1)

The Council's Scheme of Delegation, Part II (Terms of Reference of Headquarters Committees) states as a transformation function of the Economy & Infrastructure Committee that it will "Receive reports on the performance and activity of High Life Highland and Eden Court". The Scheme of Delegation will need to be reviewed to reflect the current reporting arrangements following a change in Service functions, see section 2.3 below. (See Action Plan Reference: M2)

2.2 *Identification, creation and oversight of ALEOs*

The audit objective was partially achieved. Whilst Council agreed to reduce the funding to Eden Court in 2018/19 there was no current service agreement in place to confirm the amount of Council funding and the services to be provided by Eden Court. An exchange of emails between the former director of care and learning and the chief executive of Eden Court formed the basis of the current arrangement. (See Action Plan Reference: M3)

There have been changes to the HLH service provision including the transfer of the Music Tuition Service and a change in the performance assessment methodology. Each of these changes were agreed by the Council but not formalised in a change to the Service Delivery Contract (SDC). A full review of the HLH services has not been undertaken since the contract commenced in 2011. (See Action Plan Reference: M3)

2.3 *Monitoring of ALEOs*

The audit objective was substantially achieved. The monitoring of HiTrans demonstrated that the Council was achieving good value from its funding contribution. The impact of the pandemic has meant that strict monitoring of ALEOs against the relevant agreement/SDC has not been possible. However, client officers have continued to meet regularly with the management of each ALEO, received relevant financial/performance information and monitored the associated risks. The SDC contains a clause requiring the detailed monitoring of HLH costs, which is not being undertaken and may no longer be required. (See Action Plan Reference: M3)

High level monitoring of HLH is undertaken through the presentation of six-monthly progress reports to the Council's Education Committee. During the review period no reports have been presented to any committee for Eden Court. (See Action Plan Reference: M2)

3. Conclusion

3.1 The Council has effective arrangements for governing its significant Arms Length External Organisations and Partnerships. Full assurance is achievable when compliance with all constitutional documents and all updated agreements is demonstrated.

4. Action Plan

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
M1	Medium	The Corporate Governance Team hold information on each ALEO but there is no summary register available as required by Finance Regulation 26.3. that includes the following: • The name of the organisation • The relationship to the Council • Members representing the Council • The Lead Officer representing the Council • The extent of funding including any in kind assistance • The nature of shareholding/ ownership • Name/contact details of Company Secretary	Responsibility for the maintenance of a central register of ALEOs should be allocated and reflected in the Council's Financial Regulations. A central register of ALEOs should be maintained and include: • The name of the organisation • The relationship to the Council • Members representing the Council • The Lead Officer representing the Council • The extent of funding including any in kind assistance • The nature of shareholding/ ownership • Name/contact details of Company Secretary.	Financial Regulations have been updated to reflect the allocation of responsibility to the Monitoring Officer. As noted much of the information is held and maintained in Corporate Governance.	Corporate Audit and Performance Manager Head of Corporate Governance	Complete 30/04/22
M2	Medium	Within the Council's Scheme of Delegation, the functions of the Economy and Infrastructure Committee include: "receive reports on the performance and activity of HLH and Eden Court". The Scheme is scheduled for review (expected December 2021) as it reflects the previous arrangement that saw managing the relationship with both ALEOs sitting with the ECO Transformation. Whilst HLH have	The appropriate ECO should ensure that the performance and activity of Eden Court is reported to the appropriate committee in accordance with the revised/updated Scheme of Delegation.	The need to amend the Scheme of Delegation is agreed and the annual review will be considered at Council in March 2022. Forward planning for Education Committees will include incorporation of appropriate reporting relating to Eden Court performance and activity.	Head of Corporate Governance ECO – Education and Learning	31/03/22 30/06/22

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
		been reporting regularly to Education Committee, no reports are routinely received at committee for Eden Court.				
M3	Medium	**Eden Court:** The previous funding agreement expired on 31 March 2019. Funding and service provision for Eden Court (2019 - 2022) has been based upon an exchange of emails between the former director of care and learning and the chief executive of Eden Court. The chief executive was new to Eden Court in 2019 and it is understood that he sought time to review and develop a new Eden Court Business Plan before an updated agreement between the parties was in place, which means that only basic financial/ programme information is supplied to and reviewed by the Council. **HLH:** There have been changes to HLH service provision (01/04/2018: Transfer of Music Tuition Service, 30/05/2018: other new services transferred since 2011, 05/12/2019: Performance based on Corporate Plan 2019-22), which may require a formal change to the Service Delivery Contract (SDC). The SDC (Clause 16) specifies some detailed information to be provided and reviewed to ensure	Management should ensure that: • written agreements between the Council and its ALEOs (HLH and Eden Court) fully reflect the Council's objectives, funding provided and the services being delivered; • ALEOs provide the required financial information (HLH and Eden Court) and performance information (Eden Court), which the Council reviews and monitors in accordance with the written agreements; and • periodic reviews of the ALEOs are undertaken (particularly longer term ALEO - HLH) to ensure that they remain fit for purpose and demonstrates that this is the best service delivery option for the Council.	**Eden Court** – the new Chief Executive of Eden Court starts in the role March 2022 and the Council will engage in early discussion around establishing a new Service Agreement with the Theatre. With a target date of 6 months to conclude a new agreement. **HLH** – A review of the HLH Service Delivery contract will be taken forward. The scope and timetable will be developed along with HLH Officers. The review will take place in the early part of 2022 with review recommendation and a revised SDC following thereafter. With a target date of a new SDC in place no later than 6 months into the new financial year.	ECO – Education and Learning ECO – Education and Learning	31/10/22 31/10/22

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
		HLH is not being over-compensated. A full review of HLH has not been undertaken since 2011.				

AGENDA ITEM 4ii

Internal Audit Final Report

Transformation Service

Cyber Security

Description	Priority	No.
Major issues that managers need to address as a matter of urgency.	High	1
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	2
Minor issues that are not critical but managers should address.	Low	0

Audit Opinion

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Reasonable Assurance** can be given in that whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Distribution:
Executive Chief Officer – Communities and Place
Head of ICT and Digital Transformation, Transformation
ICT Operations Manager, Transformation
ICT Transformation Managers, Transformation
ICT Solutions Architect, Transformation
Executive Chief Officer – Resources and Finance
Head of HR, Resources and Finance
Executive Chief Officer – Performance and Governance
Corporate Communications Manager, Performance and Governance

Report Ref: HDD04/004
Draft Date: 17/11/21
Final Date: 25/01/22

1. Introduction

1.1 Cyber security is defined by the National Audit Office as "the activity required to protect an organisation's computers, networks, software and data from unintended or unauthorised access, change or destruction via the internet or other communications systems or technologies".

1.2 The audit examined the Council's cyber security arrangements, including a review of the Council's Public Sector Network (PSN) compliance status and also progress made with the actions set out in the Public Sector Action Plan (PSAP) and any subsequent requirements set out by the Scottish Government (SG).

At an operational level, cyber security is a core contractual responsibility of Wipro and therefore the way in which contract performance is monitored was reviewed.

The governance framework in place to establish how decisions are made relating to cyber security and how risk in this area is managed was also looked at.

ICT changes made to enable staff to work from home due to COVID-19 were assessed to establish whether the associated cyber security risks had been appropriately mitigated.

2. Main Findings

2.1 *Control framework*

This objective was partially achieved. The National Cyber Security Centres '10 Steps to Cyber Security' guidance aims to help organisations manage their cyber security risks. By adopting security measures covered by the 10 Steps, organisations can reduce the likelihood of cyber-attacks occurring and minimise the impact when incidents do occur. The audit found that the Council's cyber security arrangements were satisfactorily aligned with the NCSC guidance in 8 out of 10 categories.

Step	Description	Satisfactory?
1	Risk management (See section 2.2)	No
2	Network security	Yes
3	Engagement and training	No
4	Malware prevention	Yes
5	Removeable media controls	Yes
6	Secure configuration	Yes
7	Managing user privileges	Yes
8	Incident management	Yes
9	Monitoring systems and networks	Yes
10	Home and mobile working	Yes

In terms of engagement and training. there is a mandatory Information Management e-learning module which covers some components of cyber security, but a previous audit carried out in 2019 identified that only 19% of employees had completed the training. A Cyber Security Awareness Session was made available to all staff in September 2018, but uptake was low and since then there has been no systematic action taken to ensure that awareness of cyber security risks is maintained amongst staff. However, the Communications and Resilience team are currently facilitating training sessions for senior managers and once these have taken place the plan is to deliver wider communications and training to all staff. There has been a recent improvement in communications to staff with a section on cyber security included in Staff Connections. The aim is to drip feed key messages to staff in future issues (See action plan H1).

The Council does not have a specific policy regarding cyber security, but there is a section within the 'Acceptable Use Policy' (AUP), which covers security matters. It was last updated in 2015 (See action plan M1).

There is a robust system in place to monitor Wipro's contract performance and this includes cyber security matters. Service Delivery review meetings are held at an operational level weekly and at a more strategic level on a monthly basis with outstanding issues continually monitored.

The Council's PSN compliance status expired in August 2020 but because of the disruption caused by the pandemic, leeway has been given by the awarding body. An independent IT health check is required prior to applying for PSN compliance and this was completed in 2020 and 2021 with remediation work carried out meaning that no serious issues were overlooked. An application

will be submitted in due course once final checks have been completed.

The PSAP was published by the Scottish Government in November 2017 and its aim was to ensure that Scotland's public bodies had in place a common baseline of good cyber resilience practice. The Council fulfilled all of its obligations under the PSAP.

2.2 *Governance and risk management*

This objective was partially achieved. At an operational level, cyber security is a core contractual responsibility of Wipro and therefore most of the mitigation measures associated with managing operational cyber security risks are outsourced to them e.g., regular patching of workstations and servers, regular updating of Anti-virus and patching of Network systems and Firewalls. There is an effective governance framework in place to monitor this activity and the associated risks (See section 2.1).

At a corporate level, Cyber Security is part of risk CR2 (Security and Resilience) within the Corporate Risk Register (CRR). This risk is considered to be above the accepted risk appetite and therefore requires active management. The level of activity (mitigating actions) required to effectively manage the risk is set out in the CRR. However, the actions focus on the technical aspects of managing cyber security risk and do not pick up on wider elements such as human behaviour and staff training and awareness.

Work is underway to bring the core ICT Service inhouse (Project Dochas) and after April 2022 the Council will have greater responsibility for the management of operational risk relating to cyber security. A new ICT Strategy (2021 to 2026) has been drafted to take account of the new delivery model. It sets out the proposed governance structure and states that the ICT Strategy Board will maintain overview of Council ICT and cybersecurity risks including making decisions on the mitigation of any escalated risks. With cyber security at the core of the new ICT Strategy, additional posts have been created to ensure that risks are effectively managed. A complete review of cyber risk is also planned, at corporate, service, and operational level (See action plan M2).

2.3 *Homeworking*

This objective was fully achieved. There were 2 key changes made in order to allow staff to work from home:

- Change of system used to remotely access the Council's network to resolve capacity and performance issues - Microsoft Always-On VPN was introduced to replace Microsoft Direct Access for Windows 10 devices
- Access to Office 365 permitted from personal devices.

Additional guidance regarding the above and also a 'Staff Briefing: Information Security when Working from Home' was issued to staff and can be found on the Intranet. Any risks associated with these changes were recorded on the 'THC-Wipro Shared Risk Register' and appropriate mitigating action taken where required.

3. Conclusion

3.1 All of the expected technical controls were found to be in place in line with NCSC guidance. However, a study by IBM found that human error was a major contributing factor in 95% of all cyber security breaches. This means that even with the appropriate technical controls in place, without adequate staff training and awareness, the chances of Highland Council falling victim to a successful cyber-attack are increased. The audit found that staff engagement and training was an area of particular weakness and one that needs to be improved.

3.2 Although there is nothing to suggest that the risks associated with cyber security are not being adequately managed, they need to be reviewed and updated in line with the new ICT Strategy and Project Dochas with emphasis given to ensuring there are appropriate mitigating actions in place.

3.3 The Council's policy regarding cyber security, which is included within the AUP, has not been updated since 2015. Although this does not necessarily mean that it's not still fit for purpose, it would benefit from a review and refresh.

4. Action Plan

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
H1	High	• The mandatory Information Management e-learning module covers some components of cyber security, but a previous audit in 2019 found that only 19% of employees had completed it • Since a Cyber Security Awareness Session was made available to all staff in September 2018, there has been no systematic action taken to raise awareness of cyber security risks amongst staff • The Communications and Resilience team are currently facilitating training sessions for senior managers and once these have taken place the plan is to deliver wider communications and training to all staff.	(i) The existing Information Management e-learning module should be reviewed to ensure that it adequately covers all aspects of cyber security.	ICT Services will provide relevant content relating to cyber security to feed into a new cyber security module on the Council's e-Learning Management System.	Head of ICT & Digital Transformation	31/03/22
			(ii) Consideration should be given to ways in which levels of awareness of cyber security matters can be raised amongst staff. This should include, but not be limited to: • Appropriate training given as part of induction process • Mandatory refresher training scheduled at regular intervals i.e., annually • Placing restrictions on access to the network or key systems unless mandatory training is completed • Regular direct communications with staff.	As per management agreed action H1(ii) (HDD04/001 Review of Information Management Arrangements), a review of the staff induction process and mandatory training should be carried out and brought back to ELT for consideration.	Head of HR	31/05/22
M1	Medium	The AUP has a specific section relating to security and was last updated in 2015.	The existing policies covering cyber security matters should be reviewed and updated in line with the new ICT Strategy. Consideration should be given to a specific cyber security policy in order to strengthen the key	The ICT Acceptable Use Policy will be reviewed and updated as required in line with the ICT strategy.	Head of ICT & Digital Transformation	22/06/22

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
			messages to staff and therefore raise awareness.			
M2	Medium	• Cyber Security is part of a wider Security and Resilience corporate risk • The mitigating actions focus on technical aspects of risk management rather than wider elements such as human behaviour and staff training and awareness • At an operational level, most of the mitigation measures associated with managing operational cyber security risks are currently outsourced to Wipro but this is due to change when core ICT services are brought inhouse over the coming months.	(i) A review of cyber risk at corporate, service, and operational level should be carried out and updated in line with Project Dochas and the new ICT Strategy. This should include consideration given as to whether cyber security should be a standalone corporate risk.	• A review of cybersecurity risks will be carried out at a corporate level with addition of a separate corporate risk for cybersecurity. • An ICT risk register will be maintained covering technical and operational ICT elements of cybersecurity. • Service risk registers and business continuity plans will be reviewed in the context of cybersecurity.	Head of ICT & Digital Transformation Head of ICT & Digital Transformation ECO's	31/03/22 31/03/22 31/01/22
			(ii) The mitigating actions should be updated to reflect not just technical measures but also wider elements such as human behaviour and staff training and awareness.	• Update any relevant technical mitigation measures • Update any relevant non-technical mitigation measures.	Head of ICT & Digital Transformation Head of HR	31/03/22 31/03/22