The Highland Council

Agenda Item	**22**
Report No	**RES/ 20/14**

Resources Committee
28th May 2014

Internal Audit – Data Handling and Security

Report by Head of Digital Transformation

Summary

The Internal Audit Review of Data Handling and Security was recently considered by the Council's Audit and Scrutiny Committee. This report is now presented to this Committee for their consideration as part of the corporate governance process.

1. Background

1.1 The purpose of this report is to update the Members of Resources Committee on the findings of the internal audit review of Data Handling and Security. The audit was undertaken as part of the annual audit plan for 2013/2014 and was reported to the Audit and Scrutiny Committee on 27th March 2014.

1.2 The scope of the Review Data Handling and Security included locations classified as data centres sites which hold server equipment and Council data of significance.

1.3 The Council's ICT contractor, Fujitsu Services Ltd, has an independent certificate of assurance for information security management to cover the main data centres holding Council data at Stevenage and also a backup facility in London. In addition, data is also held on servers at two sites in Inverness, one Fujitsu site and another owned by the Council, with a further Council site used to store backup tapes for server configuration.

1.3 Visits to the Stevenage and Inverness sites were carried out and observations on physical and environmental security for each site compared to ICT standards and best practice guidance for data centres.

2. Review Objectives

2.1 The objectives of the review were to ensure that:

(i) Assessment and management of risk is carried out

(ii) External environmental controls are satisfactory

(iii) Personnel access to these sites is controlled

(iv) Internal environmental controls within the data centre sites are satisfactory.

3. Findings

3.1 The first objective was achieved in the reviewed areas. The Stevenage Data Centre was designed and purpose built and no areas of security weakness were identified during the visit. The Inverness sites were not designed specifically as data centres but some areas of good practice were found for all sites and one area where recommendations for improvement have been made in relation to inventories of ICT equipment.

3.2 The second objective was mainly achieved, with numerous examples of good practice identified relating to security of buildings. Three areas for improvement were recommended for the Inverness sites.

3.3 The third objective was fully achieved in the areas reviewed.

3.4 The fourth objective was partially achieved, with four areas where improvement is recommended at the Council owned site, relating to lighting, heating ventilation and air conditioning systems and lack of water detectors, with the latter being a shortcoming at all of the Inverness sites.

3.5 The full Action List is attached as Appendix 1.

4. Conclusion

4.1 This review found **Substantial Assurance** with the identification of eight recommendations, 7 rated at medium and one at low grade. Of all the eight recommendations, three have already had agreed actions completed; the remaining five are in progress to be completed by April 2015.

Recommendation

The Committee are invited to note the Internal Audit Review its action plan, and that appropriate actions are being taken to address all the recommendations contained therein.

Designation: GIS Analyst, ICT Delivery Manager

Date: 6th May 2014

Author: Alastair Clinkscale, Linda Johnstone

4. ACTION PLAN

The Action Plan contains 8 recommendations as follows -

Description	Priority	Number
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	7
Minor issues that are not critical but managers should address.	Low	1
Total recommendations		**8**

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.1.2	Medium	**Asset inventory and Assessment of risk:** Inventories of equipment for data sites were provided in 2013 by ICT Services. One data site also contained primary infrastructure assets for core operational processes.	The inventories of equipment for the data sites should continue to be maintained and updated for change to allow for the assessment and management of risk and protection planning, as advised in the standard BS ISO/IEC 27005:2011 IT Information security risk management.	Changes to inventories are captured in the CMDB as part of the Change Management process. An annual risk assessment to be carried out by ICT Services, Business Support and HaPS.	ICT Delivery Manager, ICT	30/04/15
3.2.2	Medium	**External Perimeter** All three Inverness sites were developed within standard office buildings and did not exist as an inner sanctum with security zones surrounding the data hall. Therefore, external perimeters were not secured to ideal standards for information processing facilities.	Whilst it is satisfactory that there are either plans for or actual monitoring of sites by CCTV, it is recommended the external perimeter of site B is assessed for improved security in line with importance of the site, in particular walls and windows.	The external perimeter of site B will be risk assessed for security by ICT, Business Support Services and HAPS.	ICT Delivery Manager, ICT, Operations Manager (HQ) and Head of Property	30/04/15
		Fire Controls A visit to the site B found that stacked				

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.2.3	Medium	storage boxes were blocking the access to the main door area on the floor area marked to be kept clear for safe exit in the event of fire.	Responsible Premises Officer should continue to ensure regular monitoring of the site B external access area is carried out for reduction of known fire hazards and confirmation that the fire exits are clear.	Regular checks for obstructions and potential fire hazards by Business Support officers	Responsible Premises Officer/ Operations Manager, BS Finance	complete
3.2.4	Low	**Keys** Although access could be gained to site C by the key held by Fujitsu Services, Council officers could not locate a key for this area which holds backup of server data.	There should be a key on Council premises to access the site C as required	ICT will contact Fujitsu Services to obtain a Council key.	ICT Operations Manager, ICT	31/08/14
3.4.3	Medium	**Lighting and cabling** In Council site B, fluorescent lighting on the ceiling is suspended across and above the metal cable trays used to hold numerous fibre optic/network cabling and servers on racks in cabinets beneath. This does not comply with standards for IT generic cabling systems. It also creates a potential health and safety hazard to the maintenance officer managing the lighting. The officer is advised to get help from a second officer when carrying out lighting maintenance using ladders on site. The potential risk of electromagnetic interference from this non-compliance is unknown.	In the event of the data site B being re-designed in future, improved compliance to cabling design standards is recommended. A second Council officer should always be available to assist with any lighting maintenance for site B for health and safety reasons.	Noted for information - As part of any future site re-design, up-to-date design standards to be applied. A second Council Officer is available to assist with lighting maintenance for site B.	N/A Operations Manager, BS Finance	N/A complete

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.4.4	Medium	**Heating ventilation and air conditioning systems (HVAC)** Two HVAC systems at Council Site B have passed their expected average lifespan and one is reported as unreliable. The gas coolant used, R22 is being phased out as it does not comply with the EU Ozone Depleting Substances (ODS) Regulations in 2014. HAPS are drafting a new contract to re-tender for managing and servicing equipment, including the HVACS now.	As a priority, the new contract for managing the HVAC fixed equipment should be completed to ensure compliance to EU Ozone Depleting Substances (ODS) Regulations. Until remote monitoring is in place for the data centre environment it is important that a manual regular check is made for security of the IT equipment to ensure the air environment is adequately controlled.	Two HVAC units in site B to be replaced. Monthly inspection schedule to be agreed by ICT Services.	Head of Property, HAPS ICT Delivery Manager, ICT	31/08/14 Complete
3.4.5	Medium	**Server racks and cabinets** The cabinets with server racks in site B did not have the doors closed to protect the equipment. The site looked untidy in general. Data room environments have potential risk from dust fragments polluting metal structures such as cabling trays	Server cabinets in site B should be checked by ICT Services to ensure they are secured and cabinet doors closed to reduce any risk of damage. The data centre should be regularly inspected and improved housekeeping standards required of the third parties who access the site in line with CPNI guidance for data centres.	Monthly joint inspection schedule to be agreed by ICT Services and Fujitsu Services.	ICT Delivery Manager, ICT	Complete

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.4.6	Medium	**Potential water hazard** No water detectors were found at the three sites. Site A in Fujitsu premises is on the first floor underneath the roof space. Council sites B and C were both on the ground floor. Site B has a cement base with a culvert in one corner has to allow cables out of the site underground. There were also pipes on site and it was not known how much water if any ran through them.	The potential risk of water to this site should be investigated further and any pipes found to contain water be sealed or moved away from the IT equipment.	Downpipe to be checked to confirm if a grill is in place to help prevent blockage and any likelihood of flooding	Assistant Property Manager (South), HAPS	31/03/14

Appendix 1

Internal Audit Opinion

Level	Definition
Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.
Substantial Assurance	While there is a generally a sound system, there are 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.
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
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.
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.