Agenda Item	7
Report No	AS/15/16

The Highland Council

Audit and Scrutiny Committee – 29th September 2016

Internal Audit Reviews and Progress Report – 07/06/16 to 20/09/16

Report by the Audit & Risk Manager

Summary

This report provides details of the final reports issued since the previous meeting of this Committee; work in progress and other information relevant to the operation of the Internal Audit section.

1. Audit Reports

1.1 Final Reports

There have been 5 final reports issued in this period as referred to below:

SERVICE	SUBJECT	OPINION
Corporate Development	Third Party Arrangements in Relation to Information Security	Reasonable
Corporate Development	SharePoint	Reasonable
Corporate Development/ Finance	Personnel Recruitment Process	Reasonable
Development & Infrastructure	Renewable Heat Incentive (RHI) Scheme Income (Members only report)	Reasonable
Finance	Debtors	Reasonable

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.

2. Other Work

2.1 In addition to the reports referred to in the table at section 1.1 above, the Section has been involved in a variety of other work which is summarised below:

(i) Work has been undertaken on behalf of the Valuation Joint Board and the Pension Fund.

(ii) The Housing Benefit Count testing, which was reported to the last Committee as an adjustment to the audit plan has been completed and the results provided to Audit Scotland.

(iii) The corporate fraud work includes acting as the Single Point of Contact (SPOC) for liaising with the DWP's Single Fraud Investigation Service (SFIS), and investigating any fraud referrals received.

3. Staffing Issues

3.1 The Section is now fully staffed with the appointment of a former Performance Officer into the post of Assistant Auditor from 20/07/16.

3.2 Sickness absence during the period June to early September has impacted upon the capacity of the Corporate Fraud Team. This has not affected the audit plan which contains an allocation of time for investigations. However, some fraud referrals had to be put on hold as it is important that information is corroborated during an investigation, which requires two officers to be involved at particular stages. Nevertheless, some housing tenancy fraud referrals and a suspected fraudulent housing grant application have been progressed with the assistance of different Housing Officers who have provided this corroboration.

4. Progress Against the 2016/17 Plan

4.1 The audit reviews that are in progress and which will be the subject of a future report to this Committee are shown in the table at **Appendix 2**. At this stage, no adjustments to the audit plan are considered necessary.

5. Performance Information

2016/17 Quarter 1 performance is provided in the tables below.

5.1 Internal Audit:

Category		**Performance Indicator**	**Target**	**2016/17 Actuals**			
				Q1	**Q2**	**Q3**	**Q4**
Quality							
Client Feedback	(i)	% satisfaction from individual audit engagements expressed through Client Audit Questionnaires (CAQ)	90	80	-	-	-
	(ii)	% of Client Audit Questionnaires returned	70	86	-	-	-
Business Processes							
Timeliness of Final Report	(iii)	% of draft reports responded to by client within 20 days of issue	85	38	-	-	-
	(iv)	% of final reports issued within 10 days of receipt of management response	90	89	-	-	-

Commentary on the above is provided as follows:

(i) A total of 7 CAQs are referred to in the performance indicators above, 6 of which were returned.

(ii) Only 3 of the 8 audit reports issued received a timely response. The new Reporting & Escalation Protocol which came into effect from 30/05/16 is expected to bring about improvement in this area and this will be monitored accordingly with any issues escalated to senior management.

(iii) 7 out of the 8 final reports were issued on time and the last one was delayed as the response to the draft report was received after the report author had left the Section through Voluntary Redundancy. Pressure of other work meant that it took longer than expected to issue the final report.

5.2 Corporate Fraud:
The table below gives details of the number and types of fraud referrals made to the Corporate Fraud Team in the quarter together with the cumulative for the year. In considering this information, the following should be noted:

- The cumulative total is all cases closed during this quarter which includes referrals from previous periods.
- Closed cases include those where no fraud was established which could be due to insufficient information to support the fraud allegation, allegations made with good intent as well as allegations are found to be malicious.
- The number of cases which had a successful outcome is shown in brackets and this amounted to 10 cases comprising of 9 housing tenancy and 1 CTR.
- The value for the tenancy fraud for 2016/17 is £39,000 which is based upon figures provided by Audit Scotland which includes £18,000 as the sum associated with housing a family in homeless accommodation for a year and £21,000 for void periods and the necessary repairs required before the property can be re-let.

Fraud Type	**No. of referrals**				**Closed in Qtr 1**		**Cumulative closed**	
	Q1	Q2	Q3	Q4	No.	Value £	No.	Value £
Tenancy	26	-	-	-	11 (7)	273,000	14 (9)	351,000
Council Tax Reduction (CTR)	2	-	-	-	1		9 (1)	218
Non Domestic Rates	1	-	-	-	0	0	0	0
CTR & Tenancy	3	-	-	-	2	0	3	0
Total	**32**				**14**		**26**	**351,218**

6. Implications

6.1 There are no Resource; Legal; Equalities; Climate Change/Carbon Clever; Risk, Gaelic and Rural implications as a direct result of this report.

Recommendation

The Committee is invited to consider the Final Reports referred to in Section 1.1 above and note the current work of the Internal Audit Section.

Designation:	Audit & Risk Manager
Date:	20th September 2016
Author:	Donna Sutherland, Audit & Risk Manager

Appendix 1

Internal Audit – Planned Work in Progress

SERVICE	SUBJECT	PROGRESS
Care & Learning	Integrating Care in the Highlands	Terms of Reference issued
Care & Learning	Review of Throughcare and Aftercare Services	Being planned
Care & Learning	Review of the provision and maintenance of sports pitches	Being planned
Care & Learning	Review of Financial Procedures operated in Schools	Being planned
Care & Learning/ Corporate Development	Network Capacity Management in Schools	Fieldwork complete
Chief Executive's Office	Common Good Funds – rental income	Draft report in progress
Community Services	Housing Rents	Draft report issued
Community Services	Review of the arrangements for the procurement and payment of Homeless services	Fieldwork in progress
Community Services	Review of Burials and Cremations	Terms of Reference issued
Community Services	Roads Maintenance – condition surveys	Being planned
Corporate Development	Transformation Savings Programme Projects	Fieldwork in progress
Development & Infrastructure	Rental income	Fieldwork complete
Development & Infrastructure	Control of road bonds & enforcement of planning conditions	Fieldwork in progress
Development & Infrastructure	Compliance with the Carbon Reduction Commitment Energy Efficiency Scheme 2015-16	Being planned
Finance	Matters arising from the Statement of Internal Control 2015/16	Draft report in progress

The Highland Council
Comhairle na Gàidhealtachd

INTERNAL AUDIT

FINAL REPORT

CORPORATE DEVELOPMENT SERVICE
THIRD PARTY ARRANGEMENTS IN RELATION TO INFORMATION SECURITY

AUTHOR

David Beaton
Internal Audit
Finance Service

DISTRIBUTION

Depute Chief Executive & Director Corporate Development
Director of Care and Learning
Director of Development & Infrastructure
Head of Digital Transformation, Corporate Development
ICT Operations Manager, Corporate Development Service
ICT Service and Performance Manager, Corporate Development
ICT Strategy and Engagement Manager, Corporate Development
ICT Information and Records Manager, Corporate Development
Head of Resources, Care and Learning
Head of Planning & Building Standards, Development & Infrastructure
Audit Scotland [for information only]

REF: HBA01/006

DRAFT DATE: 04/04/16
FINAL DATE: 20/06/16

Contents

1. INTRODUCTION

This audit was undertaken as part of the 2015/16 Internal Audit Plan. The Highland Council's approach to the management of information security is defined in its Information Security Management System (ISMS) which was approved by the Information Management Governance Board on 2 September 2013. The Highland Council ISMS is based upon the information security international standard ISO/IEC 27001:2005 and the implementation of its associated controls defined in ISO/IEC 27002:2005. Newer versions of the standard, namely ISO 27001:2013 and ISO 27002:2013 have been since released.

The purpose of this report is to record the findings of a recently completed audit review of third party arrangements in relation to the information security guidance in Chapter 15, entitled Supplier Relationships, of the information security standard ISO 27002:2013. This chapter contains two main sections which deal with a) ensuring the protection of the Council's information which is accessible to its suppliers and b) ensuring an agreed level of security is maintained during service delivery by its suppliers.

The audit review forms part of both the Council's compliance with the ISO 27002:2013 standard and the operation of its ISMS. Chapter 18.2 of the standard, entitled Independent Review of Information Security, advises:
"the organisation's approach to managing information security should be reviewed independently at planned intervals....such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function".

2. REVIEW OBJECTIVES

The objectives of the review were derived from the 5 sections of ISO 27002, Chapter 15 and were to ensure that:

(i) Information security requirements for mitigating the risks associated with the supplier's access to the organisation's assets are agreed with the supplier and documented in a policy (section 15.1.1).

(ii) All relevant security requirements are established with each supplier that may access, process and store, communicate, or provide IT infrastructure components for the Council's information (section 15.1.2).

(iii) Agreements with suppliers include requirements to address information security risks associated with information and communications technology services and product supply chain (section 15.1.3).

(iv) The Council regularly monitors, reviews and audits supplier service delivery (section 15.2.1).

(v) Changes to the provision of services by suppliers should be managed taking into account the criticality of the business information, systems and processes involved and re-assessment of risks (section 15.2.2).

3. SCOPE, METHOD & COVERAGE

The scope of the audit included a review of:

- The ICT Services policies and procedures to control third parties services
- The third party information security clauses in the Council's main ICT Services Contract and a sample of three software contracts for computer applications, namely the Pensions System, the Education Management Information System (MIS) and the Planning and Building Control System.

- The Council's monitoring arrangements to ensure information security terms and conditions are being adhered to in the above third party contracts
- How changes to information security arrangements in contracts with third parties are managed.

4. MAIN FINDINGS

The main findings of the review, referenced to the above review objectives, are as follows.

4.1 Information Security in Supplier Relationships

The detailed guidance in the standard in relation to Section 15.1, Information Security in Supplier Relationships, is as follows.

The overall objective of Section 15.1 is to ensure protection of the Council's assets that are accessible by suppliers. This objective is broken down into three sub-objectives which correspond to first three audit objectives (i) to (iii) detailed in section 2 above. The standard also identifies three corresponding controls with respect to these three objectives, namely:

(i) Section 15.1.1 - information security requirements for mitigating the risks associated with the supplier's access to the Council's assets should be agreed with the supplier and documented.

(ii) Section 15.1.2 - all relevant security requirements should be established with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.

(iii) Section 15.1.3 - agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

4.1.1 Information Security Policy for Supplier Relationships

This objective was partially achieved. Section 15.1.1, referenced in section 4.1 (i) above, contains more detailed guidance including:

- Identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, whom the Council will allow to access its information
- A standardised process and lifecycle for managing supplier relationships
- Defining the types of information access that different types of suppliers will be allowed and monitoring and controlling the access
- Minimum information security requirements for each type of information and type of access as the basis for individual supplier agreements
- Processes and procedures for monitoring adherence to established information security requirements for each supplier
- Types of obligations applicable to suppliers to protect the organisation's information
- Handling incidents and contingencies associated with supplier access including the responsibilities of both the Council and suppliers
- Awareness training of personnel involved in acquisitions
- Awareness training of personnel interacting with supplier
- Conditions under which information security requirements and controls will be documented
- Managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring information security is maintained throughout the transition period.

The standard also states with regard to the first control (i) that information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a need for confidentiality of the information, non-disclosure agreements can be used. The Council needs to be aware that the legal or contractual responsibility for protecting information remains with the Council.

The review found that, although the ISMS should have been reviewed annually and updated to take into account the revised guidance in the 2013 versions of the ISO 27001 and ISO 27002 standards this has not yet been carried out. Section 8.2 in the ISMS, entitled 'Addressing Security in Third Party Agreements', states:

> *"Within the two main ICT agreements…..we assure that the agreement covers all relevant security requirements. Any services delivered under these contracts must comply with the contractual obligation and any specific requirements will be captured under the Service Descriptions.*
>
> *The electronic versions of our ICT Supplier agreements can be found on the ICT Services SharePoint site and Highland.gov.uk. The Service Descriptions register and services can be found on the …SharePoint site. The Council's legal department safe keeps all original signed agreements.*
>
> *For any contracts that are not managed by the ICT Services supplier, the contracts will be held and managed by the System Owner and a copy provided to ICT Services."*

The review also established that, although there are some supplier controls set up within the Council's ICT Services Contract and with respect to the Council's data in applications reviewed, there is no overarching Council policy on information security for third parties that covers all the controls detailed above.

With regard to non-disclosure agreements, the ICT Services Contract contains a confidentiality section stating that each party shall not disclose the other party's confidential information. The Pensions System Application Services Provider Agreement and the Planning and Building Control System Call Off Agreement both contain non-disclosure sections, however the Education MIS Licence Agreement does not.

4.1.2 Addressing Security within Supplier Agreements

This objective was partially achieved. With reference to the second control in section 4.1 (ii) above that all relevant security requirements should be established with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the Council's information, the ISO 27002 standard provides further implementation guidance including a statement that supplier agreements should be established and documented to ensure there is no misunderstanding between the Council and the supplier regarding both parties' obligations to fulfil relevant information security requirements. It details terms that should be considered for inclusion in the agreements. The terms include the following:

- A description of the information to be provided or accessed and methods of providing or accessing the information
- Classification of information according to the Council's classification scheme
- Legal and regulatory requirements including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met

- The obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing.

The findings relating to the second control are that some security requirements are established in the supplier agreements examined, but there is no recorded check to ensure that all relevant security requirements, as defined by the standard, are established.

In respect of the ICT Services Contract and the 3 applications examined, the following was identified:

The ICT Contract, Section 65, Security Requirements, states the supplier shall comply with the Council's Security Policy. In addition Schedule 18, Section 3 obliges the supplier to develop, implement and maintain the Security Plan to apply during the term of the Contract. The Security Plan is approved by the Council, tested, periodically updated and audited. The Security Plan, which is based on ISO 27001 and 27002 controls, was reviewed and audited in 2014. However, the security plan relates to Council security as opposed to the supplier's security. It does not provide a description of the methods of providing or accessing Council information. Schedule 18, Section 5 also states:

> *The Contractor shall be responsible as set out in this Agreement for the security of the Contractor Managed Estate and shall at all times provide the level of security which…complies with ISO/IEC27002 and ISO/IEC27001*

The Council's ICT Services supplier has provided an ISO 27001 compliance certificate for the two data centres it uses to store Council data. The ICT Services Contract also contains a security plan, but this is mainly to address the Council's information security arrangements as opposed to the supplier's information security arrangements.

In some cases, e.g. the purchase of an off-the-shelf application, the Council must accept the supplier's terms and conditions. The security requirements contained in the 3 application license agreements reviewed are as follows:

1) The Pensions System Application Services Provider Agreement states that the supplier will ensure adequate physical security is in place including a secured computer room for the servers with access controlled by a key and limited to authorised personnel. It also states that the supplier will provide security management for the system. In addition the Pensions System supplier holds an ISO 27001 information security compliance certificate.

2) The Education MIS Members Agreement covers the use of Education MIS software. A new Services Agreement is to be issued. There are also security clauses in the license agreement for the use of the Caird Street Data Centre provided by South Lanarkshire Council and the Saughton Data Centre provided by the Scottish Government. Both of these data centres are used to host the Education MIS. One is used to hold the live version and one is used to hold the back-up version. The Education MIS supplier is working towards obtaining an ISO 27001 information security certification. This concern has already been identified in the Information Security in Schools audit which was previously carried out and an audit recommendation has been made to remedy this.

3) The Planning and Building Control System was purchased via a Crown Commercial Service call off agreement. This contains a section entitled '5.6 Security' which states that the Council shall provide the supplier upon request copies of its written security procedures and shall afford the supplier upon request an opportunity to inspect its physical security arrangements, i.e. it seeks to control the customer as opposed to the supplier. The Agreement did

not mention the supplier's security arrangements however, the supplier does hold an ISO 27001 information security compliance certificate.

4.1.3 Information and Communication Technology Supply Chain

This objective was partially achieved. The additional guidance relating to control (iii) above is that agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain. Again the ISO 27002 standard details further terms for inclusion these agreements. These terms include:

- Requiring that the suppliers propagate the Council's security requirements throughout the supply chain
- Requiring that the suppliers propagate appropriate security practices throughout the supply chain
- Implementing a monitoring process and acceptable methods for validating that the delivered products and services are adhering to the stated security requirements
- Obtaining assurance that critical components and their origin can be traced throughout the supply chain
- Defining rules for sharing information regarding the supply chain.

This guidance also states that the Council works with its suppliers to understand the supply chain and any matters that have an important impact on the products and services being provided. These services include cloud computing services.

Although Section 39, entitled Supply Chain Rights, of the Council's ICT Services Contract provides some detail of how the supply chain is controlled, it does however not fully address the above guidance.

With regard to the three applications reviewed, the Pensions System Application Services Provider Agreement contains a section entitled, 'Sub-Contracting and Assignment', the Education MIS License Agreement contains a section entitled 'Assignation and Sub-Contracting' and the Planning and Building Control System Call-Off Agreement contains a section entitled 'Transfer and Sub-Contracting'. These sections do not address the above guidance either.

4.2 Supplier Service Delivery Management

The overall objective of Section 15.2 of the ISO 27002 information security standard is to maintain an agreed level of information security and service delivery in line with supplier agreements. This objective is broken down into two sub-objectives which are objectives (iv) and (v) detailed in section 2 above. The standard also identifies two corresponding controls for these two objectives, namely:

(iv) Section 15.2.1 - the Council should regularly monitor, review and audit supplier service delivery.

(v) Section 15.2.2 - changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

4.2.1 Monitoring and Review of Supplier Services

This objective was partially achieved. The ISO 27002 standard details how the control (iv) relating to section 15.2.1 should be implemented. Its states that monitoring and review of supplier services should ensure that the information security terms and conditions of agreements are being adhered to and that information security incidents and problems are properly managed. This should involve a service management relationship process between the Council and the supplier. This supplier management relationship process should include activities to:

- Monitor service performance levels to verify adherence to agreements
- Review service reports produced by the supplier and arrange regular progress meetings as required by these agreements
- Conduct audits of suppliers, in conjunction of review of independent auditor's reports, if available, and follow-up on issues identified
- Provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures
- Review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered
- Review information security aspects of the supplier's relationships with its suppliers.

With respect to this control it was established that main ICT Services Contract is monitored in a number of ways by ICT Services as defined in the Contract. Schedule 8 of the Contract defines service levels the supplier must achieve. It also states the supplier must monitor its performance against each of the service levels and produce a monthly service delivery report. The Contract Performance Report contains details of service delivery including sections on service performance, information security and information security incidents, changes via change control notice and customer satisfaction. The progress of new projects is monitored via the ICT Development Board.

Information security incidents are recorded on the supplier's helpdesk system and reported to the Council's ICT Security Group. ICT Services staff can access and review this system. Information security risks are reported to the Information Management Governance Board. In order to provide network services within the ICT Services Contract some supplier staff members require administrator access to the Council's network. This means they have access to all the Council's information held on the network. In addition some of the supplier's staff members also have access to Council applications in order to support them. The ICT Services supplier has provided an ISO 27001 compliance certificate for their two data centres located in Stevenage and the London Docklands. The ICT Services Contract also contains a security plan, but this is to address the Council's arrangements as opposed to the supplier's information security arrangements.

In terms of the 3 supplier application contracts, supplier access to carry out maintenance to the system requires to be requested.

However, there are no corporately defined arrangements for the Council's network or applications which fully address the above guidance.

4.2.2 Managing Changes to Supplier Services

This objective was partially achieved. The ISO 27002 standard details how the control in 15.2.2 should be implemented. Its states changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. It advises that the following aspects should be taken into consideration:

- Changes to supplier agreements.
- Changes made by the Council to implement:
    - Enhancements to the current services offered
    - Development of any new applications and systems
    - Modifications or updates of the Council's policies and procedures
    - New or changed controls to resolve information security incidents and to improve security.
- Changes in supplier services to implement:
    - Changes and enhancements to networks
    - Use of new technologies
    - Adoption of new products or newer versions/releases
    - New development tools and environments
    - Changes to physical location of service facilities
    - Change of suppliers
    - Sub-contracting to another supplier.

The standard also states that the Council should retain sufficient overall control and visibility of all security aspects for sensitive and critical information or information processing facilities accessed, processed or managed by a supplier.

With respect to control (v) relating to section 15.2.2 above that changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks; it was established that changes are monitored in the main ICT Services Contract via schedule 34, The Change Control Procedure, which sets out the procedure for dealing with contract changes. With respect to the three applications examined:

- The Pensions System Application Services Provider Agreement contains a change control section.
- The Planning and Building Control System Crown Commercial Service Call Off Agreement contains a section on variation which is effectively change control.
- The Education MIS Members License Agreement covers the use of Education MIS software also contains a section on variation.

However, it is questionable whether Council has retained sufficient overall control and visibility of all security aspects for sensitive and critical information or information processing facilities accessed, processed or managed by a supplier. For example, a recent PSN IT Security Health Check report identified a significant number of issues which need to be addressed.

5. CONCLUSION

The most important finding from this review is that, although there are some individual controls on third parties in place, there is no overarching policy to ensure all the risks associated with supplier's access to the Council's information are mitigated by all the controls identified in the ISO 27002 standard.

As a result of the audit five recommendations medium grade have been made. All of these have been accepted by management and the final agreed action is due to be implemented by 31/05/17.

6. 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.

7. ACTION PLAN

The Action Plan contains **5** 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	5
Minor issues that are not critical but managers should address.	Low	0
Total recommendations		**5**

REPORT REF.	**GRADE**	**FINDING**	**RECOMMENDATION**	**MANAGEMENT AGREED ACTION**	**IMPLEMENTATION**	
					RESPONSIBLE OFFICER	**TARGET DATE**
4.1.1	Medium	The review found that: (1) The Council's ISMS has not been reviewed annually to reflect the latest ISO 27001:2013 and ISO 27002:2013 guidance.	(1) The ISMS should be reviewed and updated to reflect the latest guidance.	(1) The ISMS will be reviewed and updated as required.	ICT Service and Performance Manager	31/05/17
		(2) Although there is supplier controls set up within the Council's two main ICT contracts and with respect to the Council's data in specific applications, there is no overarching Council policy on information security for third parties which covers all the controls detailed in section 15.1.1 of the ISO 27002:2013 standard.	(2) An overarching Council policy on information security for third parties which covers all the controls detailed in section 15.1.1 of the standard should be produced.	(2) The Information Security Standards will be defined for new ICT Contracts.	ICT Service and Performance Manager	31/05/17

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.1.1 (cont'd)		(3) The Education MIS Licence Agreement does not contain a non-disclosure section.	(3) The Education MIS supplier should be contacted to establish whether a written agreement about non-disclosure exists elsewhere. If not, then one should be created.	(3) The Council will contact SEEMiS LLP to clarify the position regarding non-disclosure, and if necessary make a formal request for incorporation within agreements. Any change to LLP agreements would require agreement of all 32 Local Authority partners.	Head of Resources, Care and Learning	31/08/16
4.1.2	Medium	The review found that: (1) Some security requirements are established in the supplier agreements examined, but there is no recorded check to ensure that all relevant security requirements, as defined by the standard, are established.	(1) There should be a recorded check that all relevant security requirements, as defined by section 15.1.2 of the standard, are established.	(1) The Information Security Standards will be defined for new ICT Contracts with the relevant Service Owner within Services responsible for performing the necessary checks.	ICT Service and Performance Manager	31/05/17

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.1.2 (cont'd)		(2) In some cases, e.g. the purchase of an off-the-shelf application, the Council must accept the supplier's terms and conditions.	(2) If it is not possible to enforce the Council's terms and conditions the relevant system implementation project board should be alerted by the corresponding project team to the fact that Council terms and conditions are not in place. The project team should also provide an assessment of the associated risks regarding any of the Council's terms and conditions which are not in place.	(2) The Information Security Standards will be defined for new ICT Contracts with the relevant Service Owner within Services being responsible.	ICT Service and Performance Manager	31/05/17
		(3) Although the supplier of the Planning and Building Control System has an ISO 27001 compliance certificate, the Call Off Agreement does not refer to the supplier's security arrangements.	(3) The supplier should be contacted to discuss and identify its security arrangements to ensure they are adequate.	(3) This will form part of the agenda at the next account meeting with the supplier (IDOX) which is attended by ICT and D&I officers, The outcomes and any subsequent changes required will be assessed and implemented in consultation with the ICT Service and Performance Manager.	ICT Service and Performance Manager/ Head of Planning & Environment, Development & Infrastructure	31/05/17

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.1.3	Medium	The ICT Services Contract and the three application contracts reviewed do not address the supply chain guidance defined in the standard.	There should be a recorded check in future contracts to ensure that all relevant supply chain controls, as defined by section 15.1.3 of the standard, are established. If it is not possible to implement these controls because it is necessary to accept the supplier's terms and conditions, the relevant project team should notify the relevant project board and assess the associated risks.	The Information Security Standards will be defined for new ICT Contracts with the relevant Service Owner within Services being responsible to perform the necessary checks.	ICT Service and Performance Manager	31/05/17
4.2.1	Medium	There are no corporately defined arrangements for the Council's network or applications which fully address the standard's guidance with respect to monitoring and review of supplier services.	ICT Services should produce a corporate policy and procedures for monitoring, reviewing or auditing supplier service delivery in accordance with the standards guidance.	As part of the new ICT target operating model we will define operating standards for ICT service owners.	ICT Service and Performance Manager	31/05/17
4.2.2	Medium	Given the results of the recent PSN IT Security Health Check report, it is questionable as to whether the Council has retained sufficient overall control and visibility of all security aspects for sensitive and critical information or information processing facilities accessed, processed or managed by a supplier.	ICT Services should review its overall control and visibility of all security aspects for sensitive and critical information or information processing facilities accessed, processed or managed by a supplier.	We will establish the capability for ICT Services to carry out independent monitoring.	ICT Operations Manager	31/05/17

The Highland Council
Comhairle na Gàidhealtachd

INTERNAL AUDIT
FINAL REPORT

CORPORATE DEVELOPMENT SERVICE

SHAREPOINT

AUTHOR

Norma Duncan
Internal Audit
Finance Service

REF: HBA01/004.bf

DISTRIBUTION

Depute Chief Executive & Director of Corporate Development
Head of Digital Transformation, Corporate Development for info
Head of People and Transformation for info
Corporate Improvement Project Manager, Corporate Development for info
Information & Records Manager, Corporate Development for info
Audit Scotland for info

DRAFT DATE: 14/07/16
RE-DRAFT DATE: 12/08/16
FINAL DATE: 19/09/16

Contents

1. INTRODUCTION

The audit was undertaken as part of the 2015/ 16 audit plan and reviewed controls in place for the Microsoft [MS] SharePoint platform for managing and sharing information in the Council. Currently SharePoint versions 2007, 2010 and SharePoint Online are in use, although SharePoint Online is only used to a very limited extent.

The Council's Information Management Strategy dated February 2015 refers to the SharePoint 2010 platform as playing a key part of the Council's Information Architecture through having tools and technical controls to support the management of information and records. The Council's Record Management Plan refers to it as one of a line of business IT systems having some records management functionality. The Plan states that SharePoint [SP] does not fully meet the requirements in recognised standards such as 'MoReq' to be a full Electronic Document Records Management System [EDRMS]. However, it could become one with the purchase of a system add-on.

The SharePoint 2010 server infrastructure internal to the HC domain, storage components and software are managed within the main ICT contract by Fujitsu Services for the Council. A corporate SharePoint Administration Team within ICT Services manages sites and liaises with the service provider.

During the audit review, the Council's Managing Information Project was rolling out the use of SharePoint as part of a wider programme of work with teams to improve information management practices, assisting in the transfer of data off network folders onto the SharePoint platform where appropriate.

2. REVIEW OBJECTIVES

The objectives of the review were to ensure that:

(i) Policies in place provide adequate controls for SharePoint

(ii) Procedures and training are available for SharePoint users

(iii) Security controls are in place for user access, site access ownership and authorisation

(iv) There are appropriate arrangements in place for the security of data including a policy for site content consistency, controls for classified data, metadata controls, version controls and an adequate audit trail is maintained

(v) There are secure arrangements for the management of change, including the review of data retention and removal of out of date information.

3. SCOPE, METHOD & COVERAGE

The audit examined controls on the use of the SharePoint versions 2007 and 2010, thereafter referred to as SP2007 and SP2010, taking account of controls and best practice in the international standards ISO 27001 & 2:2013 for Information Security and other guidance on how to manage the SP environment.

The method used to collate evidence included interviewing officers including the Corporate Managing Information Project Manager, the Information and Records Manager and the SP Administration Team's Technical Business Analyst. Reference to system documentation and documentation for the Managing Information Project was also included.

The audit takes into account the service continuation agreed with Fujitsu for managed ICT Services up to 31st March 2017 and ICT re-provision planning.

4. MAIN FINDINGS

The main findings of the review, referenced to the above review objectives, are as follows:

4.1 SharePoint Service Policy Documents

This objective was partially achieved as three service policy documents are out of date or have not been finalised. These included the following:

4.1.1 The Service Description document dated 31/05/12 with the contractor's agreed levels of service support for SP including configuration, change and release management, capacity planning, volumetrics and dependencies for service delivery was out of date. For example, volumes for the agreed service quoted:

'*A maximum intranet user population of 6,500 intranet users*' with '*My-site personal storage space of 50Mb*'.

This storage capacity is a tenth of the secure storage for users for Office Desktop Services in the Office Services contract.

The agreed service also included:

'An *extranet user population of 118 registered partners'*.

The agreed service did not directly provide Disaster Recovery or Business Continuity but this could be requested as a service by the Council.

This Service Description stated it was to be reviewed annually to ensure the service continued to meet the Council's requirements. However, as outlined above, this has not been done.

4.1.2 The High Level Design document for the SP2010 farm, which defines the design and infrastructure of SharePoint servers for sharing common resources, is out of date. The SP farm included 11 servers with 1 for extranet deployment of SP for collaboration with external Council partners. It was reported that the SP2010 extranet option was not in use, therefore the server infrastructure for this extranet access was not being utilised.

The document listed topics to be addressed for the information architecture in Low Level Design documentation as required, for example Council customisations such as Corporate workflow design and storage of e-mails as records.

4.1.3 At the time of the audit, the current Model for the SP platform was not documented and approved by the relevant officers. An agile approach was being used through the MI Project to learn about the platform for an approach to site design. Changes to the model over time have resulted in SP sites being set up differently depending on the model in use at the time of implementation. For example, some SP sites had no named Site Owner assigned (see section 4.3.2).

4.2 Procedures & Training

This objective was partially achieved as:

- The contractor for the SharePoint service was responsible for pro-active monitoring and management of the Council's network under its direct control to ensure the service has appropriate resources to meet the Council's business requirements
- The Council's SP Administration Team have delegated system administration access to all HC sites. HC Site Owners for each SP site can choose to devolve administration of their site to another as required
- There was resource in place for the rollout of new SP 2010 sites through the MI Project and formal rollout procedures for creating new SP service sites were provided. For example, a sign off process was documented and the SP

Administration Team reviewed new sites to ensure they met the site structure of the current model. Transfer of data from network folders onto new SP Team sites was defined within five gateway stages and progress was reported to the Information Management Governance Board [IMGB]
Training was provided to new users by the MI Project Team officers including a Training Guide, SP Administration Team Site Guidance for Services and Dealing with Shared Drives

- The contractor provided the Council's SP Administration Team with quota usage reports on a semi-regular basis. Site owners also receive reports with warnings when their sites come close to their quota limit.

4.2.1 The Secure Operating Procedures document, called SP Information Security, defined security requirements for the development, management and use of SP2010 in line with the Information Security standard and best practice. This procedures document is not used as a live document and is out of date. Procedures detail included business continuity, access controls, security classification and audit logging. For example, SP is defined as business critical. The procedures document reported that the Council would define appropriate Service Level Agreements [SLA] for business continuity and content recovery which Fujitsu would be responsible for carrying out. These were to include recovery point objectives and recovery time objectives defined by the Council. However, SLAs with these recovery objectives were not found during the audit review. The agreed SP service description document did not include disaster recovery or business continuity although Storage Area Network [SAN] replication was described as being in place if required.

No agreed documented procedures were found for the Council's SP administration Team who have site collection administration tasks at lower tier or sub-site level.

The security classification levels for documents in the secure operating procedures document was described as an optional data field. If this column is left blank, the document would be unclassified. This could potentially create a risk where a document which should have protective marking is not marked manually to identify this.

4.2.2 Metadata or 'data about data' assists in the consistent labelling and categorisation of documents stored in SharePoint. The Council is not utilising the "managed metadata" enterprise function in SP2010.

Metadata is used on libraries and controls are applied manually on a library by library basis based on an assessment of the information being stored. Where the metadata is set up as compulsory, it is not possible to fully add a document to a library without metadata being applied.

4.3 Access controls

This objective was partially achieved as the following controls are in place:

There is separation of duties between the SP farm access, site collection and site levels as follows:

- The contractor accesses and manages the SQL Server database and carries out database administrator roles according to the SLA requirements
- Site Collection administrator level access is limited to the Council's SP Administration Team
- Site level access requires users to be set up within an SP User Group.

The Council is responsible for creating users and managing their properties, including which groups they belong to and what they are authorised to do.

Site Collection is the responsibility of the Council and the design and initial configuration is managed by the SP Administration Team. Primary and Secondary

Site Collection Owners are to be set up when new sites are created as part of the latest rollout of SP2010.

User access and permission is determined locally by each Site Owner and provided by the SP Administration Team. Once set up, Team Site Groups & Responsibilities can be viewed within the SP site by all site users and provide security assurance.

During the audit it was initially established that there was no SP access control policy documented. This was addressed in line with ISO27002 section 9.1.1. and an approved access control policy for SP was produced dated 11/04/16.

4.3.1 The Information and Records Manager is the responsible officer for SP2010. However, there is no named responsible officer for SP2007 which is an older, unsupported version and is not being actively managed. Twenty SP 2007 sites are listed as still active and of the 32 named site owners, 12 are no longer employed by the Council.

4.3.2 It was reported by a Technical Business Analyst in the SP Administration Team that a number of SP2010 sites had no assigned Site Owner; this had occurred either through being started before the current site development process was agreed or because of changes in staff. The number of these was not specified. These sites are being reviewed by the SP Administration Team, which is updating sites to ensure they have Site Owners while implementing the current permission group structure.

4.3.3 Roles can be allocated to users either directly or through SharePoint Security groups, Active Directory groups or a combination of both. The SP Administration Team have delegated System Administration access and can create user groups with permissions as required by the Site Owners who define sets of permissions on discrete parts of a site by role. The Council only used three Active Directory groups within SharePoint groups.

No complete list of all user groups created in SP was found. The approach to creating groups was described in the access control policy document that was produced during the review. The IS Security standard ISO27002 recommends maintaining a central record of access rights granted to user IDs to access information systems and services as best practice.

4.3.4 Changes to Users' access requirements, including leavers, were reported as being the responsibility of the SP Site Owner, who should be the Information Asset Manager. However, this responsibility is not included in the Role Description for Information Asset Managers.

It was reported that for changes to access within a team, authorisation can be given verbally; outside of the team it should be by email. This process was defined as the best approach by the system manager however the risk with verbal approvals is that there is no documented audit trail.

4.3.5 The authentication of SP users is by MS Windows for the Council's network for normal users and those with higher privileges, with regular synchronisation to Active Directory to confirm a user's access. The IS Security standard ISO27002 recommends greater access controls for users with higher privileges, however there is no reference in the Council's Information Security Management System [ISMS] Password Policy rules or Information Security Policy to guide higher privilege users towards increased controls.

4.4. Security of data

This objective was partially achieved as:

- Each Council SP Team site has its own structure based on the team's functions. The local site owner can change permissions for those who can access the site with read only and contribute permissions. Higher level permissions are set by the SP Administration Team

- The creation, editing and deletion of documents are controlled at a local level through the controls put in place for each document library
- ICT Services are responsible for Site collection administration. The site collection permission allows full access for site collection administrators to everything within the site collection even where inheritance is broken which provides corporate oversight
- The Council File plan or Business Classification Scheme was planned for implementation in a separate Records Management System
- Version control for Document Lists and Libraries is not enabled by default. It was reported that versions are available to switch on for specialisms as required. This can assist in storing, tracking, and restoring items in a list and files in a library whenever they change.

4.4.1 A technical review of the SP2010 platform was commissioned by the contractor from an external consultant and a report provided in October 2015 on Due Diligence of the SP2010 Environment. This report described 10 findings where improvements could be made. These were defined as follows; 2 critical findings which had to be addressed, 7 recommended findings that should be addressed and 1 non-urgent with a lower risk of impact. It was reported that these were still being reviewed by the contractor.

4.4.2 Site Collection administrators can set up audit reports on items including changes to permissions, items that have been deleted or restored and changes to auditing settings.

However, audit log reports are not utilised by the SP Administration Team. This was reported to be due to restrictions on space on the SP 2010 platform.

The SP2010 product provides limited log details for documents and reports the date and time audit detail when a user input, created or modified a document on SP2010 sites.

For administrator and operator logs, this does not comply with the Council's Information Security Management System [ISMS] which states that:

'*Auditable events will be carefully selected to minimise overheads but will include a record of all significant system change…*' and ' *System administrator and system operator activities should be logged and should be reviewed on a regular basis*.'

The Council's Record Management Plan - Element 11 refers to the audit trail detail applied to Council records. This Plan stated that the Council uses SharePoint for filing electronic records which is not a full EDRMS, but could become one with the purchase of a system add-on. The new electronic store on the Council's network drives for holding records is controlled through a manual process administered by Records Management, with an audit trail maintained once records have been deposited. This element has been identified by the Keeper who reviews Record Management Plans for compliance to the Public Records (Scotland) Act as requiring further work to meet the expected standard. Reports on progress against the Plan are provided to the Council's IMGB as this is regularly reviewed.

This gap has still to be addressed with the addition of Electronic Document & Records Management technology. However, with a new ICT contract due to commence in early 2017, it is not considered appropriate to progress the procurement of an ERMS and this was reported to the IMGB on 13/04/16.

4.5 Security Management of Change

This objective was partially achieved. Capacity Management reports were provided by the contractor to the Council's SP Administration Team as agreed in the SLA which states: '*service will pro-actively monitor and manage all components of the Council's Network under Fujitsu's direct control to ensure that the SharePoint Platform service has the appropriate resources to meet the current business requirements of the Council in cost effective and timely manner. The Service will include performance reports and system usage analysis to provide identification of negative trends, potential problems and future options to improve the performance of the service*.'

4.5.1 The SP Administration Team has permissions to remove any sites that are dormant and should be shut down. The Team can also lock down sites by making content "read only" to protect information as required. However, the administrative procedures for removing SP sites have not been documented.

During the audit it was reported to the IMGB that some applications built in to SP2010 such as the Travel Desk may not easily migrate from SP2010 to later versions of SharePoint such as SP2013, SP2016 and SP Online It was also reported that there was insufficient capacity within SharePoint 2010 to move all teams into the platform. These issues were under review in April 2016.

It was reported that there was a records management drive available as an archive repository for electronic records after they are moved out of SP2010. Guidance on transferring electronic records is available to Council Teams. The MI Project Team reported to IMGB in April 2016 that it was not currently appropriate to progress the procurement of an Electronic Records Management System due to project deliverables and timescales associated with the roll out of SharePoint subject to change, and with a new ICT contract due to commence in early 2017.

The National Archives document 'Records management in SharePoint 2010' on implementing SP2010 as a records management solution raises implications and usability issues for implementing records management in SP2010[1]. Progress on the potential solution or add-on to SP to manage this identified gap in audit trail functionality in SP is to be reported to the Keeper, who requested that he was kept informed.

4.5.2 The disposal process for information no longer required is manual, requiring Team Site Owners to review, archive and delete documents according to the Council's records management processes. There is functionality within SP2010 to automate this process if required but it is not in use as it not in keeping with records retention management.

5. CONCLUSION

The findings of the review confirm the increasing use of the SP platform as a business service to manage Council information and records. The current work of the MI Project has assisted in rollout of the platform to a wider user group within the Council. However, this rollout has still to reach all Council users.

As more information is transferred into SharePoint from network folders, it is important to review risks and controls in line with increased business requirements. For example, SP2010 is not listed as a critical system in the current ICT Service contract.

[1] NAS Records management in SharePoint 2010 (2011) is at http://www.nationalarchives.gov.uk/documents/information-management/review-of-records-management-in-sharepoint-2010.pdf

A benefit of using the SP platform is that it provides useful workflow functions for information management. If resource requirements increase in the future, a review of the potential to automate processes that are currently carried out manually would be beneficial in maintaining the SP service.

It is understood that progress to complete actions to address risks and actions will be impacted by timings of ICT re-procurement processes in the year ahead.

As a result of the audit ten recommendations have been made, one high priority grade, eight medium grades and one low grade. A number of these have multiple recommendations, all of which have been accepted by management except for one part action where it has been decided that it would be inefficient to update the SP Service Description document with the current ICT supplier as this contract is coming to an end. Three actions have already been fully completed and a further three are partially completed with the remainder due to be implemented by 30/04/17. April 2017 is also the month when the new ICT Core Services contract comes into operation.

6. 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.

7. ACTION PLAN

The Action Plan contains **10** recommendations as follows:

Description	**Priority**	**Number**
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	8
Minor issues that are not critical but managers should address.	Low	1
Total recommendations		**10**

REPORT REF.	**GRADE**	**FINDING**	**RECOMMENDATION**	**MANAGEMENT AGREED ACTION**	**IMPLEMENTATION**	
					RESPONSIBLE OFFICER	**TARGET DATE**
4.1.1 – 4.1.3	Medium	SP documents are out of date including: (1) The contractor's agreed levels of service in the Service Description as the SP service has changed/ evolved.	(1) The Service Description document should be updated, agreed and authorised for SP service provision.	(1) With the ICT contract coming to an end and a new contact being awarded the Service Description will not be further updated. The current SharePoint platform will be replaced.		No action
		(2) The architectural High Level Design document for the SP Farm refers to extranet deployment; however, this is not being used.	(2) The SP High Level Design documentation should be updated, agreed and authorised.	(2) A review is underway by Fujitsu and any important changes that are required will be made. Due to timing as above few changes are expected.	Information & Records Manager	30/04/17
		(3) The current SP Model has not been fully documented. Changes to the model have resulted in SP sites being set up differently depending on the model in use at the time.	(3) The current SP Model should be documented and signed off. A review of SP sites should be completed to ensure they comply with the current model.	(3) The documentation for the SharePoint model has been completed and signed off.	Information & Records Manager	Complete

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.2.1	Medium	The Secure Operating Procedures document for SP Information Security has not been reviewed since 2012 and is not a live document. No documented procedures were found for the Council's SP administration Team who have site collection administration tasks.	Documented SP procedures should be reviewed and updated for usefulness, including consideration of procedures for site collection administration and business continuity and content recovery processes.	The documentation for the SharePoint model has been completed and signed off.	Information & Records Manager	Complete
4.2.2	Low	Metadata is applied manually by the Council on a library by library basis.	Should resource requirements for managing metadata become problematic, this process could be reviewed.	This will be taken into account if such a situation was to arise in the future.	Information & Records Manager	Complete
4.3.1 - 4.3.2	Medium	There is no named responsible officer to manage SP2007 sites. Twenty SP2007 sites are listed as still active and of the 32 named site owners, 12 are no longer employed by the Council.	There should be a named responsible officer for SP2007 sites and documented procedures for reviewing old sites for archive/ deletion.	The SharePoint 2007 platform is in the process of being removed. Until sites are removed a named officer has been identified - Information & Records Manager.	Information & Records Manager	Complete
		Some SP2010 sites have no assigned Site Owner. These are being reviewed by the SP Administration Team along with a review of the permission group structure.	The work underway to ensure all SP2010 sites have an assigned Site Owner and the current permission group structure should be completed.	Work will be continued to ensure all sites have a site owner.	Information & Records Manager	30/04/17
4.3.3	Medium	No central record of access rights granted to User IDs in SP was found. The SP Access Control Policy provided detail on SP Administrator accounts, SP Developer Accounts and SP groups and core permissions for site level access. The Information Security standard ISO27002 recommends that a central record of access rights granted to User IDs is maintained.	Consideration of the usefulness of maintaining a record of user IDs should be made, as this would provide a central record of access rights and comply with best practice requirements of ISO27002, section 9.2.2.	This has been considered and no further action is required. The information is available centrally to site collection administrators. This ensures that this information is 100% accurate, not subject to human error and avoids duplication of effort.	Information & Records Manager	Complete

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.3.4	Medium	(1) Responsibility for notifying changes to site users' access requirements, including leavers is the responsibility of the SP Site Owner, or Information Asset Manager. However, this is not included in the Role Description for Information Asset Managers.	(1) Information Asset Managers' responsibilities for SharePoint should be included in their Role Description.	(1) The role description for the Site manager will be reviewed to ensure it fully covers this responsibility. Not all Information Asset Managers will be responsible for a SharePoint site so it is not relevant to add it to the role description for the IAM.	Information & Records Manager	30/04/17
		(2) It was reported that within a team site, authorisation for changes can be given verbally. The risk of verbal approvals is that these cannot be traced in an audit trail in the event of any failure of access.	(2)Consideration should be made of recording authorisation for team sites in writing as a log e.g. as an email.	(2) This has been considered and will not be implemented due to the undue burden on services. The controls in place to ensure appropriate access controls are adequate.	Information & Records Manager	Complete
4.3.5	Medium	User Authentication is by login to MS Windows for the Council's network for all users including those with higher privileges.	Controls for users with higher privileges in SP should be strengthened in accordance with ISO 27002. The use of increased controls for higher privilege users could be included within the Council's ISMS Password Policy rules	The ISMS Password Policy will be updated to cover the increased controls that should be in place for users with higher privileges.	Information & Records Manager	30/04/17

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.4.1	High	A report on security of the SP2010 Environment issued in October 2015 contained 2 critical and 7 recommended findings to be addressed. It was reported that at the time of the audit review these were being reviewed with the contractor.	Action should be taken to address the report findings ensuring that the 2 critical findings are prioritised and addressed, followed by review/ completion of the 7 recommended findings.	A review of the findings is being undertaken by Fujitsu and any changes deemed necessary by the Council will be implemented.	Information & Records Manager	30/04/17
4.4.2	Medium	Audit reports are available for Site Collection administrators but are not utilised due to restrictions on space on the SharePoint 2010 platform. The SP product provides limited audit log details and reports every occasion a user modifies a document by date and time.	Audit reports should be reviewed for usefulness for areas considered highest risk in accordance with good practice standards and policy. For example, the 'Changes to auditing' report would assist in compliance to the ISMS for audit logging.	A review will be carried out of the available audit reports and a decision made as to whether any of these should be utilised.	Information & Records Manager	30/04/17

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.5.1 - 4.5.2	Medium	(1) For SP2010 to become a full EDRMS there is a need to manage the archiving of records. Progress on the potential solution or add-on to SP to manage the identified gap in records management functionality in SP is to be reported to the Keeper, who requested that he was kept informed. The MI Project Team reported to the IMGB in April 2016 that it was not currently appropriate to progress the procurement of an Electronic Records Management System due to project deliverables and timescales associated with the roll out of SharePoint subject to change, and with a new ICT contract due to commence in early 2017.	(1) The Keeper should be kept informed of the archive process for SP documents which are records in line with the Council's Record Management Plan and the Public Records (Scotland) Act 2011.	This will be done in accordance with our obligations under the Public Records (Scotland) Act 2011.	Information & Records Manager	01/04/18
		(2) Disposal processes for old information no longer required are manual, with Team Site Owners reviewing archiving and deletion of documents according to the Council's records management processes. As in 4.2.1, procedures used by the SP Administration Team for removing SP sites no longer required have still to be documented.	(2) Procedures for the deletion of SP sites should be documented and all SP site disposals should be logged for operational purposes.	(2) SP documentation will be updated to cover the process for the retention and disposal of SharePoint sites.	Information & Records Manager	30/04/17

INTERNAL AUDIT

FINAL REPORT

CORPORATE DEVELOPMENT SERVICE/
FINANCE SERVICE

PERSONNEL RECRUITMENT PROCESS

AUTHOR

Yvonne Holmes
Internal Audit
Finance Service

DISTRIBUTION

Director of Finance
Depute Chief Executive/ Director of Corporate Development
Director of Care & Learning
Head of Revenues & Business Support, Finance Service
Business Support Operations Manager (Mid), Finance Service
Payroll & Pensions Manager, Finance Service
Head of People & Transformation, Corporate Development Service
HR Manager, Corporate Development Service
Principal Project Manager, Corporate Development Service
Head of Resources, Care & Learning ServiceWorkforce Planning & Staffing Manager, Care & Learning Service
Audit Scotland

REF: HDB08/001.bf

DRAFT DATE: 27/07/16
FINAL DATE: 20/09/16

<u>**Contents**</u>

1. INTRODUCTION

The Corporate Improvement Programme 2 (CIP2) ran between 1st April 2013 and 31st March 2015 and comprised of 8 projects with a target to achieve efficiency savings of £5.98m. One of these projects, the Business Support (BS) project, aimed to deliver efficiencies in relation to back office or support functions, in effect delivering the support the organisation required at less cost. Phase 1 of this project involved the implementation of revised personnel administration processes which aimed to deliver a more efficient, controlled and user-friendly process, in respect of Establishment, Recruitment and Contract Management. The revised processes saw the move to electronic SharePoint forms which are completed by managers and, once submitted, are automatically sent to the correct generic mailbox in BS or Payroll for processing. These processes were implemented in July 2014 and are supported by BS staff based at Human Resources (HR) Hubs in Fort William, Dingwall, Wick and Inverness. Service establishment information and all employee information continues to be recorded and updated on ResourceLink, the Council's integrated personnel and payroll system.

The National Recruitment Portal (NRP), which is operated by COSLA on behalf of all 32 Scottish Councils, is a crucial element of the recruitment process as it is used to administer all vacant posts which will be filled. In January 2015, TalentLink, a new NRP, was introduced to replace the soon to be obsolete iGrasp system. The TalentLink system is used by both BS staff and recruiting managers during the recruitment process.

2. REVIEW OBJECTIVES

The objectives of the review were to ensure that:

(i) There are documented procedures in place for the new personnel recruitment process and these are applied consistently across the Council.

(ii) The maintenance of Service Establishment information held on ResourceLink is adequately controlled and accurately reflects current Service structures.

(iii) The new personnel recruitment process has delivered the intended efficiencies.

(iv) The Council's personnel recruitment process makes full use of the TalentLink system's functionality and is adequately supported by the system.

3. SCOPE, METHOD & COVERAGE

The audit reviewed the Council's revised personnel administration processes. In particular it looked at whether or not the desired efficiencies had been achieved and a sample of 15 posts recruited between October 2015 and January 2016 were examined to assess whether or not the revised processes had been adhered to.

The system of controls around changes to Service Establishment information on ResourceLink was assessed and a sample of a change to a Service structure was checked to ensure that the appropriate adjustments had been made to the Service Establishment information held on ResourceLink.

The audit also considered the effectiveness of the TalentLink online recruitment system and whether or not current processes make the most efficient use of the system by utilising all available functionality.

4. MAIN FINDINGS

The main findings of the review, referenced to the above review objectives, are as follows:

4.1 Documented procedures

This objective was partially achieved. The revised personnel administration processes encompass a number of tasks carried out by both recruiting managers and BS staff within the SharePoint HR Portal and TalentLink system. Some training and guidance had been provided.

<u>TalentLink</u>

Training was provided when the system was first introduced in January 2015. Face to face training was delivered to BS staff and online training was made available via the 'My Online Learning' platform for end users. There are also generic guides available on the HR Portal relating to all tasks carried out within TalentLink.

<u>HR Portal</u>

There is on-screen guidance available on the HR Portal Home Page which advises users which form should be completed for each task. On-screen guidance is also available within each of the forms to assist the user with completing various fields.

4.1.1 Whilst there is some guidance available, it only covers certain aspects of the process and there is no overall guidance available which summarises the processes carried out on SharePoint. There are process maps for the recruitment process but these are out of date. However, a toolkit is currently being developed by HR that will contain a flowchart and step by step guide process. There will also be pre-recruitment guidance which will include the requirement to maintain service establishment information.

A step-by-step guide to the process on TalentLink has been prepared for Head Teachers and is currently being trialled. Feedback received so far is positive and on completion of the trial this guide will be issued to all Head Teachers.

Recruitment and selection training is not currently part of induction training for management positions with a responsibility for recruitment.

4.1.2 A sample of recently recruited posts was examined in order to establish whether or not the correct procedures had been followed in relation to completion of the various standardised online forms. Due to a lack of documented procedural guidance it was not possible to assess compliance. However, a verbal overview of the process was obtained from BS staff and the sample was assessed against this. There are a number of standard forms available via the SharePoint HR Portal site which must be completed by the recruiting manager, and then submitted electronically for processing. The forms available are as follows:

- Service Establishment Form – used to create, amend or delete an obsolete post from the Service Establishment, information updated in ResourceLink by BS (see section 4.2)
- Authority to Recruit Form – used to recruit to a new or existing post within the Service Establishment, post created on TalentLink by BS
- Interview Arrangement Form – used to specify interview slots which are then created on TalentLink by BS
- Employee Form – used to inform Payroll of an appointment to a post for a new or existing employee, or if an employee is leaving a post to move to another Service, leaving the employment of Highland Council, acting up,

moving to flexible retirement or changing personal/ contractual details. Information updated in ResourceLink by BS and Payroll.

The main issues identified related to Authority to Recruit and Employee Forms.

Authority to Recruit (ATR)

An ATR form must be completed and appropriately authorised for each vacancy where prior permission has been granted to fill the vacancy. ATR forms had been completed and authorised for all posts examined. However, a standard approach had not been taken in the case of schools whereby some forms had been completed by the Head Teacher and some by the Care & Learning Workforce Planning & Staffing section. In these cases all ATR forms should have been completed by either the Head Teacher or the school office support staff and then submitted to Workforce Planning for approval.

Employee Form (EF)

An EF should be completed for each new start and submitted to Payroll. In all of the cases examined an EF had been completed and submitted to Payroll. However, as with ATR forms, a standard approach had not been taken in the case of schools whereby some had been completed by Head Teachers, some by BS staff and some by the Workforce Planning section. In these cases, EF's should all be completed by Head Teachers.

BS staff are currently permitted to complete EFs for supply teachers and relief staff as these posts have no set manager or base. However, the sampled posts did not fall in to this category. Additional support is also provided by Workforce Planning and BS to facilitate recruitment in schools during school holidays and at other times when high levels of recruitment has to be carried out within tight timescales.

4.2 Maintenance of Service Establishment information

This objective was partially achieved. Standardised Service Establishment Forms are available via the HR Portal and these allow Services to add, amend or delete obsolete posts from their establishment. There is another element of establishment maintenance whereby posts can be linked to the appropriate line manager. This ensures that the correct reports appear under the line managers 'My People' listing within the MyView HR Payroll Portal which is used for absence recording and the submission and approval of expense claims.

A restructuring of the Transport Planning team, approved by the Planning, Development & Infrastructure Committee on 03/06/15, was examined. The following changes had been agreed:

- Move the posts currently located within Community Services as part of the Road Safety/ Safer Routes to School team into the wider Transport Planning team in the Development & Infrastructure Service
- Move the 2 Urban Traffic Management team to Community Services from the Development & Infrastructure Service.

All relevant changes had been made to the establishment and linkages had been created to the appropriate line manager.

4.2.1 There are no controls in place around who can create and submit a Service Establishment Form via the HR Portal and forms submitted do not have to be authorised. However, at a meeting of the Corporate Improvement: Business Support Project Board on the 31/03/16, the Board considered whether there should be further controls of the establishment put in place. It was decided that the overall control of establishment information should be left with the Service and that no further policing or control was required. The Board stated that

Services should ensure that existing processes and checks were being applied by way of managers ensuring that their teams were correct in ‘My People’ including vacant posts, using Service Establishment Forms on the HR Portal for any changes required, and through regular monitoring of staffing budgets through current Finance processes.

4.2.2 The linkages between posts and the relevant line manager are maintained within the ‘Hierarchy Post to Post’ module within ResourceLink. There are currently system performance issues with this module which means that BS staff find it very time consuming or sometimes impossible to update the required information. These issues have been raised at the highest level with the system provider, Northgate, and Fujitsu and the situation is being closely managed by senior officers from the Finance Service. There is currently a workaround in place which does allow the post to line manager linkages to be maintained.

4.3 Efficiencies delivered

This objective was partially achieved. The overall aim of the revised personnel administration processes was to provide a more efficient, controlled and user-friendly process, in respect of Establishment, Recruitment and Contract Management. The project also aimed to deliver a number of more specific cashable and/ or efficiency benefits, a number of which have been achieved:

- Corporate ATR being used by the whole organisation – standardised process and therefore significant reduction in effort for BS
- Improved and standardised processes to ensure that the establishment is correctly maintained
- Posts advertised online only via TalentLink which feeds into the myjobscotland website
- Tried and tested methods and approaches to change management were adopted which led to a more efficient process
- BS Superusers were identified and heavily consulted and involved during the planning and implementation which therefore led to a smoother transition.

During the course of the CIP2, the Business Support project delivered £1.225m of savings. A proportion of this was predicated on the increased standardisation and efficiency of ‘back office’ or support processes, including the new personnel administration processes. The targeted savings against these processes are understood to have been achieved.

4.3.1 However, not all of the efficiency benefits were fully achieved. A new reference policy was introduced with the aim of establishing best practice whereby references were only required to be sought for the preferred candidate as opposed to all interviewees. The exception is that references are sought for all applicants who are invited for interview to teaching posts, this is historical and discussions are on-going with Head Teachers to move away from this practice.

4.3.2 One of the efficiency benefits related to the standardisation of the recruitment process. The aim was that it should be more efficient, with BS HR Hubs able to share information and work and recruiting managers having a clearer understanding of roles and responsibilities in the process.

The development of the HR Portal on SharePoint has enabled BS HR Hubs to share information and manage workloads more effectively. The BS HR Hub staff were asked whether or not they felt that the recruitment process was more efficient than it was previously. The consensus was that the revised processes were more efficient when the correct procedure was followed, however deviation from the correct procedure often led to time-consuming workarounds.

Lead officers for the recently recruited posts referred to at section 4.1.2 were asked whether or not they felt that the recruitment process was more efficient than it was previously. While there were only 5 responses there were indications that further investigation would be beneficial. As the process owner the recently appointed Head of People & Transformation has established a cross-Service review group for the recruitment process and will ensure that this meets the needs of Services and is working as efficiently as possible.

In late October 2015, just over a year since the revised processes went live, the opportunity was taken to look at how it was working and whether or not improvements or further efficiencies could be made. A workshop was held which involved representatives from HR, BS, Corporate Improvement, Payroll, Care & Learning and Community Services and as a result, an improvement plan was put together which included a number of action points. The majority of the actions related to making the SharePoint forms easier to complete by ensuring that the required information was more readily available to recruiting managers. A number of actions have been completed and work is ongoing to complete the outstanding actions.

The Corporate Improvement Team are currently looking at whether or not the recruitment module within MyView (ResourceLink) could be used as an alternative to the current system of SharePoint forms in order to further streamline the process for recruiting managers. An extensive review of the overall recruitment process, including the current reference policy, is also being carried out by HR and this may also impact on the current processes detailed within this report.

4.4 TalentLink

This objective was fully achieved. Vacancies are created on TalentLink by BS staff on the basis of information submitted by recruiting managers on the ATR form. Forms have to be submitted by midday on a Monday in order to be advertised on the following Tuesday. There is a schedule of submission and corresponding publishing dates on the HR Portal. All of the recently recruited posts examined as part of the audit had been created by BS in TalentLink by the appropriate 'Publishing Date' as per the advertising schedule.

The BS HR Hubs were asked if they felt that TalentLink adequately supported the recruitment process and the consensus was that it did if used properly. Lead officers for the recently recruited posts at section 4.1.2 were asked the same question. 3 out of the 4 respondents felt that the system did adequately support the recruitment process although 1 commented that they didn't have the time or expertise to use it and 1 said that they did not find it very intuitive and therefore it was time consuming.

Although there is TalentLink functionality which is not currently being used, it is either not fit for purpose, does not fit within Highland Council's agreed processes or is less efficient than current methods. The way in which TalentLink is used is continually reviewed and is discussed at quarterly meetings with COSLA which are attended by representatives from HR. A health check of TalentLink is currently being arranged with COSLA and this will also involve an assessment of how the Council operates the system to see if methods can be improved. BS HR Hubs identified a number of ways in which they felt that TalentLink could be improved in order to better utilise the functionality or improve the efficiency of the process. These will be passed on to the TalentLink Project Manager for consideration and fed in to the review process as appropriate.

5. CONCLUSION

Efficiencies have been delivered with the introduction of the revised personnel administration processes. A standardised recruitment process is now in operation across all Services and the introduction of the SharePoint HR Portal has allowed Business Support to manage and share work more effectively. However, the absence of clearly documented and current guidance means some recruiting managers, particularly those who recruit infrequently, are not always clear as to what their role is within the process and how to complete the required forms properly. The introduction of the revised process would appear to have been problematic for school based users in particular and this needs to be addressed going forward.

In the short-term, work is ongoing to make improvements to the current process by means of the actions agreed at a workshop held in October 2015. In the longer-term, the wider recruitment process is being reviewed by HR and the Corporate Improvement Team is looking at an alternative system for managing the process in order to increase efficiency. Until such time as wider changes are made to processes as a result of these reviews, appropriate guidance and training has to be made available to managers so that current processes can be operated more effectively.

As a result of the audit, 4 medium grade and 1 low grade recommendations have been made. All of these have been accepted by management and the final agreed action is due to be implemented from 01/08/17 onwards.

6. 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.

7. ACTION PLAN

The Action Plan contains **5** 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	4
Minor issues that are not critical but managers should address.	Low	1
Total recommendations		**5**

REPORT REF.	**GRADE**	**FINDING**	**RECOMMENDATION**	**MANAGEMENT AGREED ACTION**	**IMPLEMENTATION**	
					RESPONSIBLE OFFICER	**TARGET DATE**
4.1.1	Medium	Whilst there is some guidance available to all users, it only covers certain aspects of the process and there is no overall step by step guide. A toolkit is currently being developed by HR. This will include revised recruitment guidance and a step by step guide to the overall recruitment process. A step-by-step guide to the process on TalentLink has been prepared for Head Teachers and is currently being trialled. Recruitment and selection training is not currently part of induction training for new managers.	(i) Revised guidance, including a step by step guide to the overall process should be made available to all users. The guidance should cover completion of SharePoint Forms and TalentLink processes. It should incorporate the TalentLink step by step guide already prepared for Head Teachers. Once available, all managers should be made aware of the guidance. (ii) Recruitment and selection training should be built in to the induction process for new managers. This should also include ensuring that access is granted to the appropriate systems.	A step by step guide and flow chart will be developed and implemented. Recruitment and selection training will be built into the induction process for new managers.	Head of People & Transformation Head of People & Transformation	30/09/16 30/09/16

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.1.2	Medium	For the recently recruited posts examined, a standard approach had not been taken in the case of schools for the completion of Authority to Recruit and Employee Forms. Authority to Recruit (ATR) Some ATR forms had been completed by the Head Teacher and some by the Care & Learning Workforce Planning & Staffing section. In these cases all ATR forms should have been completed by either the Head Teacher or the school office support. Employee Form Some EF's had been completed by Head Teachers, some by BS staff and some by the Workforce Planning section. In these cases, EF's should all be completed by Head Teachers. BS staff are currently permitted to complete EFs for supply teachers and relief staff. However, the sampled posts did not fall in to this category. Additional support is also provided by Workforce Planning and BS to facilitate recruitment in schools during school holidays and at other times when high levels of recruitment has to be carried out within tight timescales.	The role of Head Teachers within the current recruitment process should be evaluated, within the context of the Future Management of Schools Programme, and a decision made as to whether or not additional administrative support is required in this area. Whatever approach is decided upon should be applied consistently across all schools.	Action to be taken in terms of providing appropriate administrative/clerical support to Head Teachers as per the outcome of the School Office Review and on-going review of HR processes by People and Transformation. These changes will be incremental beginning in August 2017 and on-going as the Future Management of Schools Programme is rolled-out across the Council.	Head of Resources (Care & Learning)	From 01/08/17

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.2.1	Medium	There are no controls in place around who can create and submit a Service Establishment Form via the HR Portal and forms submitted do not have to be authorised. However, at a meeting of the Corporate Improvement: Business Support Project Board on the 31/03/16, it was decided that the overall control of establishment information should be left with the Service and that no further policing or control was required.	A standard approach should be taken by all Services to the monitoring of Service Establishment information. This approach should be clearly communicated to all managers and those responsible for the regular monitoring of staffing budgets.	Service Directors to be instructed to contact their Budget holders to remind them Establishment forms should only be processed by Budget Holders or nominated officer to ensure changes are aligned to budgets.	Head of People & Transformation	01/10/16
4.3.1	Low	The implementation of a new reference policy whereby references are only required to be sought for the preferred candidate as opposed to all interviewees has only been partially achieved. This is now the case for all recruited posts apart from teaching posts whereby references are sought for all applicants who are invited for interview.	The requirement to seek references for all applicants invited for interview for teaching posts should be reviewed. An assessment should be made as to whether this is still an operational requirement and discontinued if appropriate.	Following consideration of the recommendation made by People and Transformation that references should only be called for successful candidates not currently employed by the Council, this has been discussed with Head Teacher representatives and a decision made to move to this practice by the end of November 2016.	Head of Resources (Care & Learning)	30/11/16

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.3.2	Medium	One of the efficiency benefits of the revised process related to the standardisation of the recruitment process. The aim was that it should be more efficient, with BS HR Hubs able to share information and work and managers having a clearer understanding of roles and responsibilities in the process. This was only partially achieved: – The revised processes are more efficient from a BS perspective providing that all of the relevant forms are completed correctly by the recruiting manager, which is not always the case – Feedback received from 3 out of the 5 lead officers stated that they felt that the process was far less efficient than previously and quite complicated especially if it was something which they did not use frequently.	There should be joint working between HR and the CIP team in relation to the wider HR review of the recruitment process and the CIP project relating to the potential use of My View for recruitment purposes. Issues relating to the incorrect completion of ATR and EF forms and the perception from some lead officers that the current process is less efficient and quite complicated should be addressed and considered when making any changes to processes.	People & Transformation will work with Business Support and client Services to review the end to end recruitment process.	Head of People & Transformation	01/11/16

The Highland Council
Comhairle na Gàidhealtachd

INTERNAL AUDIT
FINAL REPORT

FINANCE SERVICE

DEBTORS

AUTHOR	**DISTRIBUTION**
Martin Golembiewski Internal Audit Finance Service	Director of Finance Head of Revenues and Business Support, Finance Service Head of Corporate Finance, Finance Service Head of Resources, Care and Learning Service Revenues Manager, Finance Service Audit Scotland
	DRAFT DATE: 09/06/16
REF: HDB06/001.bf	**FINAL DATE:** 08/09/16

Contents

1. INTRODUCTION

An audit review was undertaken to examine the Council's system for the control and recovery of income from Debtors in the financial year 2015/16. In the financial year 2015/16 there were 110,934 invoices raised with a value of £79.2m and 6,775 credit notes with a value of £5.7m. The total amount of sundry debt owed to the Council at 31/03/16 was £15.1m. Audit Scotland intends to place reliance on this audit.

2. REVIEW OBJECTIVES

The objectives of the review were to ensure that:

(i) The data transferred to Integra from Oracle financials was complete and accurate;

(ii) There is an adequate control framework over access to and operation of the Integra Sales Ledger;

(iii) Income is properly captured for all chargeable goods and services and recorded in the Sales Ledger in a consistent and timely manner and is complete, accurate and valid;

(iv) All payments received from valid customers are promptly processed and accurately recorded in the Integra Financials system;

(v) Debt management, arrears follow up procedures, and bad debt write-offs are properly controlled; and

(vi) Outputs from the Integra Sales Ledger are complete, accurate and valid and are produced in a consistent and appropriate format in a timely manner.

3. SCOPE, METHOD & COVERAGE

3.1 The audit examined transactions during the financial year 2015/16 and included reference to the Integra Sales Ledger system. Testing samples were selected for the Highland Council, Pension Fund, Hitrans, and High Life Highland (HLH) invoices and credit notes.

3.2 Financial Regulations section 14 details the Council's procedures for the collection of income. This section includes a guidance note called "Issue of Debtor Accounts", which describes the main principles of credit giving and invoicing.

3.3 A large number of officers were contacted as part of this audit including key personnel in the Income & Recovery Team, Accountancy teams, Finance Systems Administration Team (FSAT) as well as officers within all Services of the Council involved in the raising of sundry debtor invoices and credit notes.

4. MAIN FINDINGS

The main findings of the review, referenced to the above review objectives, are as follows:

4.1 Transfer of data to Integra from Oracle financials

4.1.1 This objective was fully achieved in that the transfer of £14.037m of balances due on invoices was transferred from the outgoing financial system Oracle to the new system, Integra, with only a £98 difference. The transfer of customer references only occurred after the project implementation team reviewed references provided by Internal Audit and excluded 268 out of 426 with the same name and address. Those duplicate references that were transferred are required due to separate references being needed where there is differing recovery profiles or payment methods, i.e. Direct Debit (DD) or non-DD.

4.2 Financial system control framework

This objective was substantially achieved in that the users for the 3 existing systems (Oracle 11i, PECOS, and Purchase Cards) were checked to ensure that they needed to be transferred before they were migrated over to Integra.

4.2.1 Although a review of system users was undertaken prior to the migration, there was no final check or reconciliation undertaken to ensure that the 1,526 users set up in Integra was correct. A reconciliation was undertaken as part of the audit review using information provided by FSAT and the Purchase Card Administrator which identified that 1,514 active users should have been set up. For the remaining 12, 10 left prior to the transfer and 2 retired during the transition period.

4.2.2 Within Financial Regulation 14 "Income, Grant Applications and Grant Claims", the Guidance Notes "Issue of Debtor Accounts" and "Receipt of Income" refer to the previous financial system. The Revenues Manager stated that he updated these Guidance Notes in November 2015 but there had been a failure to upload these to the intranet.

4.3 All income due is invoiced

This objective was partially achieved for the reasons outlined below.

A sample of 30 invoices raised for the Highland Council (26), Pension Fund (1), HITRANS (1), and High Life Highland (2) were reviewed to ensure:

- the invoice details agree to the supporting documentation;
- it was raised by an appropriate officer;
- the correct charges applied for goods/services provided by the Council;
- it was posted correctly in the sales and general ledger;
- VAT was treated correctly;
- the invoice sum was for more than £10;
- credit checks had been undertaken; and
- that invoices were raised promptly in accordance with Financial Regulations.

This identified the following issues:

4.3.1 2 invoices did not match to their supporting documents. One raised by ICT Services for HLH ICT recharges for £20,795 was £577 less than expected and another for road salt sales raised by the TEC Services Warehouse for £190,403 overcharged the customer by £8,986. This second invoice was also issued 58 days after the last delivery. A credit note has subsequently been issued to address the overcharge but only after it had been identified by Internal Audit. However, no reasons could be given for the invoice discrepancies. Another invoice raised by the Planning section for Inverness City Heritage Trust's payroll costs recharges was also found to be late with the costs for July to December 2015 not invoiced until the end of February 2016.

4.3.2 One invoice in the sample of 30 reviewed was for £8.15 and related to unpaid school meals. Financial Regulations state that invoices should not be raised for amounts less than £10 where possible. It transpires this was one of 92 invoices raised due to unsigned cheques being presented for the payment of school meals.

A further 500 invoices were also raised during last summer's school holidays for former Primary 7 (P7) pupils with school meal debts as this cannot be carried over to their secondary school account. It is envisaged by the Care & Learning's Principal Resources Officer that the volume of invoices at the end of the 2016/17 academic session will be substantially less than last year, as they have been reminding schools throughout the year that reminders must go out regularly. It is hoped that this, and improved arrangements for the central monitoring of debt on an on-going basis, will lead to an improved situation this year. Additional reminder notes were also issued out 2 weeks prior to the end of term to all pupils in P7 with outstanding debt.

4.3.3 The Guidance Note "Issue of Debtor Accounts" states that the supply of goods and services for sums over £10,000 should be subject to credit checking by the Service Finance Team. Within the sample of 30 invoices reviewed, 14 were for more than £10,000 but no credit checks were carried out. The explanations provided were that the customer was either a government or public sector agency or body, or an organisation with which the Highland Council has a contractual relationship with, but not necessarily for the item(s) invoiced. However, no such exceptions are referred to within the Guidance Note.

A sample of 30 credit notes raised for the Highland Council (27), Pension Fund (1), HITRANS (1), and High Life Highland (1) were reviewed to ensure:

- the request for a credit note originated from the relevant budget holder;
- the details agree to the supporting documentation;
- the credit amount was correct;
- it was correctly coded in the general and sales ledgers;
- any VAT was treated correctly;
- an appropriate reason was provided/recorded for the credit note and that this was not used to unofficially write-off a debt; and
- it was cross-referenced to the original invoice number.

This identified the following issues:

4.3.4 The Guidance Note "Issue of Debtor Accounts" states that *"If for the undernoted reasons, all or part of an invoice has been issued in error, the budget holder should request the Service Finance Accountant or the Exchequer Operations Manager for OPHB invoices or their delegated nominee to create a credit note for the appropriate amount and issue it to the customer".*

However, the actual practice is different. From the sample of 30 credit notes reviewed, only 8 had been requested by the relevant budget holder. The remaining 22 had not originated from the budget holder although in 8 cases they had been informed of the request by email. For the remaining 14 credit notes the budget holder was not involved. These related either to an overpayment of housing benefit (10) where the claimant went back onto benefit (and is therefore recovered from on-going benefit entitlement), or where a dummy invoice was raised for accounting purposes, as payment was by Direct Debit (4). Examples of this are school wrap around care, music tuition, and school lets. In these cases schedules are prepared and passed to the relevant Service Finance Team and the budget holder copied in.

The arrangements in place for overpaid housing benefit and Direct Debits are considered satisfactory but these do not currently comply with the requirements of Financial Regulations.

The Guidance Note also refers to 4 valid reasons why an invoice can be cancelled. These are the only acceptable reasons for a credit note to be raised. It was also noted that one credit note was raised unnecessarily as the debtor invoice had not included the Purchase Order number.

A number of other issues were also identified from the audit:

4.3.5 A review of the Highland Council Age Debt report revealed a number of occasions where the same customer had multiple invoice issued to them on the same day by the same officer, with invoice reference numbers either running sequentially or very close together which suggests that these were raised at the same time. Examples included former tenant arrears issued to the same customer for various addresses or one case where a tenant had locked themselves out on 3 separate occasions in April, May and July 2014 and 3 invoices were then raised in May 2015, which is also an unacceptable delay. Whilst there may be a valid reason for some being separate, such as different recovery methods of overpaid Housing Benefit, for most there is no reason why one invoice with multiple line descriptions could not be issued. The raising of multiple invoices to the same customer is inefficient and increases the Council's costs. Furthermore, the pre-payment or use of Direct Debits for regular monthly charges should be encouraged.

4.3.6 Despite being informed by the system supplier that there would be no gaps in transaction references, small gaps of between 1 to 3 reference numbers were found in invoices for the Council and HLH. Gaps in reference numbers were also found for credit notes and debit/ credit adjustments/ transfers. In total 56 missing invoices references were identified in 2015/16 (up to mid-March) out of approximately 116,400 references used. This issue has been raised with the supplier but has not yet been resolved. It has been suggested that this is caused by network issues as a reference number is assigned when a transaction is entered. Should the network crash prior to completing the input the data is lost but the system believes the reference number has been used so goes to the next available reference number. The potential risk is that without the ability to trace all invoices raised, an invoice could be deliberately deleted to hide fraudulent activity and its removal blamed on this technical issue.

4.3.7 The system offers the ability for users to attach scanned documents to transactions, which is currently not utilised by most users. Of the 16 transactions where an attachment authorising the credit note was expected, there was only 8 which had this information. This consisted of 5 cancellation forms signed by the budget holder and 3 evidencing that the budget holder had been informed of the cancellation.

4.4 Suspense Accounts

4.4.1 This objective was fully achieved. A total of 9 suspense accounts relate to sundry debtors. 5 of these were originally set up but have since been identified as being redundant and will need to be disabled. At the time of the audit 4 suspense accounts had not been cleared, subsequently 2 have been and the remaining 2 uncleared accounts will be carried forward and addressed during 2016/17.

4.5 Debt Management

This objective was fully achieved for the reasons outlined below:

4.5.1 Issues with the Council's ICT provider meant that no reminders for overdue debt were issued before 13/08/15 for HLH and 20/08/15 for Highland Council. These issues have since been resolved with reminders now issued in accordance with the prescribed timescales.

4.5.2 The Guidance Note "Issue of Debtor Accounts" states that *"if a commercial debt remains unpaid after 53 days, the Income and Recovery Team will after consulting with the relevant Service consider imposing interest on the unpaid debt under the Late Payment of Commercial Debts (Scotland) Regulations 2002*". However, imposing interest can only be done once the debt has been referred to Court and to date this has only occurred once.

A sample of 5 write-offs was examined and these had appropriate reasons for the write-off and were approved by an appropriate officer in accordance with the Council's Scheme of Delegation.

4.6 Integra Sales Ledger Outputs

This objective was partially achieved as:

4.6.1 A review of 7 control account reconciliations relating to the Highland Council, Pension Fund, HITRANS, and HLH showed that 3 had long standing discrepancies. The discrepancy was known but the delay was attributable to the system supplier investigating and providing a suitable solution. The Highland Council and Common Good Fund reconciliations have subsequently been resolved and cleared, with only the HLH reconciliation still having an unresolved discrepancy. It was explained that this wasn't cleared due to the time pressure of the year-end close down process but will be investigated further and cleared during 2016/17.

4.6.2 Reconciliations were previously undertaken on a monthly basis but the new system now provides daily reconciliations. The Principal Accountant was closely involved in setting these up and had maintained an overview of the process during the year. However, no formal reviews had been undertaken. It has been agreed that for the current financial year daily reconciliations will be reviewed, on a sample basis at least one a month and that this review will be recorded.

5. CONCLUSION

Overall, the receipt of income payments from Council customers is being processed on the Integra Sales ledger accurately and invoices are being raised for chargeable services provided. However, some issues have been identified with the accuracy of the amounts invoiced and invoices have not always been issued in a timely manner. A number of operational practices do not accord with the requirements of Financial Regulations and these may be out of sync with each other. Compliance with Financial Regulations is an important part of the Council's financial framework and so it is important to ensure that these reflect operational requirements whilst setting out the appropriate systems of internal control.

There are 12 recommendations made as a result of this audit, 1 high priority grade, 10 medium priority grades, and 1 low priority grade. 5 of these have been completed, and another recommendation with 2 actions has been partially completed. The remaining recommendations are due to be implemented by 31/06/17.

6. 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.

7. ACTION PLAN

The Action Plan contains **12** recommendations as follows:

Description	**Priority**	**Number**
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	10
Minor issues that are not critical but managers should address.	Low	1
Total recommendations		**12**

					IMPLEMENTATION	
REPORT REF.	**GRADE**	**FINDING**	**RECOMMENDATION**	**MANAGEMENT AGREED ACTION**	**RESPONSIBLE OFFICER**	**TARGET DATE**
4.2.1	Medium	No final check was undertaken to ensure that all users set-up on the Integra system was correct. Of the 1,514 users transferred, the audit review identified 12 users who had left the Council, 10 prior to the new system being introduced and 2 during the transition period.	Future projects which involve the migration of system users should incorporate a final check to ensure the accuracy of the numbers requiring to be set up.	Agreed.	Finance Systems & Change Manger (for Finance-owned systems)	Completed
			The 12 active users identified as having left the Council should have their system access de-activated.	Agreed.	Finance Systems & Change Manger	Completed
4.2.2	Low	Whilst the Guidance Notes which support Financial Regulation 14 were updated to reflect the system change from Oracle to Integra, these have not been updated on the intranet.	The amended Guidance Notes should be uploaded to the intranet.	Agreed.	Audit & Risk Manager	30/09/16
4.3.1	Medium	Errors were found in the sums charged for 2 of the 30 invoices reviewed. One invoice was overcharged by £8,986 and the other was undercharged by £577. In addition, the overcharged invoice and another one were issued significantly later than expected.	Services raising sundry debtor invoices should be reminded that these should be issued promptly as set out in Financial Regulations and it should be ensured that the correct amounts are invoiced.	Agreed.	Revenues Manager	Completed

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.3.2	Medium	Approximately 600 invoices, some of which were for sums under £10, were issued for unpaid school meals provided in the 2015/16 academic year.	(i) Schools should be reminded periodically to issue reminders on a weekly basis for debt under £20, unsigned cheques should be returned to parents and that they remind parents that school meals should be paid for in advance. Schools should also be reminded that school meals accounts, particularly for P7 pupils, are cleared before the end of the school year. (ii) Schools, Area Catering Offices, and Resources Teams should be reminded of the need to adhere to the School Meals Financial Procedures – Unpaid Meals Procedures.	Reminders are, and will continue to be issued to schools.	Principal Resources Officer	31/10/16
4.3.3	Medium	Financial Regulations require credit checks to be undertaken for the supply of goods and services over £10,000. However, these are not carried out.	(i) Management should revisit this requirement and amend the Financial Regulations/ Guidance Note if it is decided that checks on certain organisations are unnecessary.	Agreed.	Revenues Manager	Completed
			(ii) Where it is decided that credit checks are necessary then Services should be reminded that these should be undertaken in all cases.	Agreed.	Revenues Manager	Completed
4.3.4	Medium	The Guidance Note “Issue of Debtor Accounts” states that credit notes should be requested by the budget holder. However, the actual practice differs in cases of overpaid housing benefit and where an invoice is cancelled because payment will be made by Direct Debit.	(i) Management should revisit this requirement and amend the Financial Regulations/Guidance Note if it is decided different arrangements should apply for overpaid housing benefit and Direct Debit arrangements. Following this, Services should be instructed of the need to comply with the requirements of the Guidance Note and Financial Regulations.	Agreed.	Revenues Manager	Completed

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.3.4 cont.		An invoice has been cancelled with a credit note being raised for a reason other than the 4 acceptable reasons as set out in the Guidance Note "Issue of Debtor Accounts".	(ii) Services should be reminded that invoices should only be cancelled for the reasons set out in the Guidance Note.	Agreed.	Revenues Manager	Completed
4.3.5	Medium	Multiple invoices are being issued to customers on the same day by the same officer which is inefficient and provides poor customer service.	Services should be reminded that unless there is a valid reason to the contrary, a single invoice containing the relevant service description(s) should be issued to customers.	Agreed.	Revenues Manager	Completed
4.3.6	High	Gaps in the reference numbers of invoices, credit notes, and adjustment transactions were found which could be used to hide fraudulent activity.	The Revenues Team should continue to pursue this matter with the system supplier to obtain a solution which ensures that all reference numbers can be fully accounted for.	A request has been sent to the system supplier for an update.	Revenues Manager	31/03/17
4.3.7	Medium	Integra offers the option of attaching documents to individual transactions which can provide a useful audit trail. However, the procedure/guidance note does not clearly set out when this should be used and what documents should be attached.	The procedure/guidance note should be updated setting out when and what documents should be attached to transactions within Integra.	Agreed.	Revenues Manager	31/12/16
4.4.1	Medium	5 suspense accounts which were originally set up in have since been identified as redundant in Integra.	(i) All redundant suspense accounts should be deactivated.	The suspense accounts will be deactivated.	Principal Accountant- Accounts and Central Services	30/09/16
		Also 2 suspense accounts were not cleared and have been carried forward into the next financial year.	(ii) The uncleared suspense accounts should be investigated during 2016/17 and cleared.	These accounts will be investigated during 2016/17 with any balances treated appropriately prior to 16/17 financial year end close down.	Principal Accountant- Accounts and Central Services	30/06/17

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
4.5.2	Medium	The Guidance Note refers to imposing interest on commercial debt but this is incorrect as this can only be done after consideration by the Court.	Management should revisit this requirement and consider removing this from Financial Regulations and the Guidance Note.	Agreed.	Revenues Manager	Complete
4.6.1/ 4.6.2	Medium	3 Debtor control accounts (Highland Council, Common Good, and HLH) had known discrepancies though out 2015/16. Resolution from the system supplier was delayed but when provided this allowed the Highland Council and Common Good accounts to be cleared.	(i) The HLH debtor control account discrepancy should be investigated further and cleared during the 2016/17 financial year.	Further investigation to take place and account cleared by ledger close down at financial year end.	Principal Accountant-Accounts and Central Services	30/06/17
		Integra provides a daily reconciliation process. However, no formal review of reconciliations was undertaken by a senior officer.	(ii) A sample of daily reconciliations should be reviewed by a more senior officer during the year and this should be evidenced accordingly.	Process for monthly review of daily control account reconciliations by Principal Accountant to be instigated.	Principal Accountant-Accounts and Central Services	31/10/16