

# Scottish Sports Council Group and Lottery Fund

Annual Audit Report 2012-13

---

September 2013





## Contents

1. Executive Summary	4
2. Financial Statements	6
3. Financial Position	8
4. Governance	12
5. Performance	13
Appendix A: IT General Control Recommendations	16

# 1. Executive Summary

## Introduction

The Auditor General for Scotland appointed Grant Thornton LLP as auditors to the Scottish Sports Council (the Council) and Scottish Sports Council Lottery Fund (the Lottery Fund) under the Public Finance and Accountability (Scotland) Act 2000 for a five year period from 2012. This is the second year of our appointment. This report summarises the findings from our audit work for the year ended 31 March 2013.

## Our responsibilities

It is a condition of our appointment that we meet the requirements of the Code of Audit Practice, which is approved by Audit Scotland and the Auditor General for Scotland. The most recent Code was published in May 2011 and applies to audits for financial years starting on or after 1 April 2011.

The Code of Audit Practice highlights the special accountabilities that are attached to the conduct of public business and the use of public money. This means that public sector audit must be planned and undertaken from a wider perspective than the private sector. We are therefore required to provide assurance, not only on the financial statements and annual governance statement, but also on Best Value, use of resources and performance.

## Our Annual Report

This report summarises the findings from our 2012-13 audit of the Council and Lottery Fund. The scope of our work was set out in our Audit Approach Memorandum, which was presented to the Audit Committee on 29 January 2013.

The main elements of our audit work in 2012-13 have been:

- the audit of the financial statements, including a review of the annual governance statement
- a review of corporate governance arrangements, internal financial controls and financial systems
- a review of the Council's response to Audit Scotland's national study reports.

The key issues arising from these outputs are summarised in this annual report.

## Overall Conclusions

The key findings emerging from each aspect of our work during 2012-13 are detailed on page 5. Overall, the Council is in good financial health with a strong reserves position of £6.2 million. The Lottery Fund continues to receive substantial funding from the National Lottery Distribution Fund and reserves are £40.4 million. There have been a number of developments to the risk management framework which now need to be taken forward in 2013-14. The Trust faces a number of challenges during the following year which will test the governance arrangements. The Council has a number of initiatives which are delivering efficiencies and effectiveness in the use of its resources. Considerable efforts continue to be made, as new programmes are being developed to deliver the corporate plan, to identify core measures and how these relate to the outcomes described as the five changes in the corporate plan.

## Acknowledgements

We would like to take this opportunity to record our appreciation for the kind assistance provided by officers of the Council during our audit.

## Key Findings

Reporting Area	Our Summary
Financial Statements	<ul style="list-style-type: none"> <li>We intend to give an unqualified opinion on the financial statements of both the Council and Lottery Fund and on the regularity of transactions undertaken for the 2012-13 financial year.</li> </ul>
Financial Position	<ul style="list-style-type: none"> <li>The key source of funding for the Council is the Scottish Government. In 2012-13, the Council received grant-in-aid totalling £49.3m, an increase of £10.9m (28%) from 2011-12. The Council has a general reserve balance of £9.0m at 31 March 2013.</li> <li>The Lottery Fund's key source of income is from the National Lottery Distribution Fund. In 2012-13 the Lottery Fund received £31.5m, an increase of £6.6m (27%) from 2011-12. General reserve balance of £40.4m at the 31 March 2013.</li> </ul>
Governance	<ul style="list-style-type: none"> <li>The Council has made improvements to the risk management arrangements which will need to be embedded in the organisation during 2013-14.</li> <li>The revised Trust Board arrangements have strengthened the governance of the Trust, a number of recommendations have been agreed which will further strengthen the arrangements.</li> </ul>
Performance	<ul style="list-style-type: none"> <li>The Council has a number of initiatives which have demonstrated Best Value.</li> <li>Considerable efforts continue to be made to identify core performance measures and how these relate to the outcomes.</li> </ul>

## 2. Financial Statements

We intend to give an unqualified opinion on the financial statements of the Group and Lottery Fund and on the regularity of transactions undertaken for the financial year 2012-13.

### Financial Statements Audit

The draft financial statements were of good quality and we identified no significant errors or misstatements. The supporting working papers reflect the standard of the accounts. The 2012-13 Management Commentary was provided during the completion stage of our audit.

Our Audit Findings report which we will present to the Audit Committee on 24 June 2013 provides our detailed findings.

### Audit Adjustments

Our audit identified three minor errors in the Trust accounts. The Group draft financial statements were adjusted for one of these errors, relating to the recognition of donated income. The unadjusted misstatements related to the under accrual of year end invoices. Management have not adjusted the accounts based on materiality.

The Lottery Fund accounts included National Lottery Fund Proceeds of £30,714k based on the interim statement from the National Lottery Distribution Fund (NLDF). During the audit, the final statement from the NLDF confirmed the proceeds as £31,008 an increase in £294k from the interim statement.

A reduction in accruals relating to Regional Partnerships totalling £526k was identified in the accounts.

In addition to the financial statement adjustments, our audit also identified a small number of presentational and disclosure issues impacting the financial statements.

### Internal Controls of Key Financial Systems

Overall, the results of our interim testing confirmed that there is a sound system of internal control covering key financial systems operated by the Group and Lottery Fund.

During the interim visit we assessed the design effectiveness and walked through financial systems to confirm whether controls are implemented in line with our understanding in areas which we have identified as a key financial system which include:

- operating expenses
- payroll
- grants payments

We reviewed the journal entry policies and procedures as part of determining our journal entry testing strategy and have not identified any material weaknesses which are likely to adversely impact on the Council's control environment or financial statements.

### IT Review

We performed a design effectiveness review of IT general controls. This review covered controls around IT security, IT operations and change management. We also reviewed the IT controls surrounding the implementation of the new CRM system.

We assessed IT general controls in the Council against expected controls and best practices that have been noted in Government and other sectors.

We identified good practice in that the Council has a recovery server room in Edinburgh where data is replicated on a timely basis which would facilitate the

recovery of IT systems should a disaster affect the Glasgow server room.

We noted a number of opportunities to improve the IT control environment which are detailed in Appendix A. The recommendations are grouped under two main risk areas: unauthorised access to IT systems and inadequate management of IT changes. The latter is particularly relevant for the new CRM system as it is subject to internal customisation.

## Regularity

We did not identify any instances of irregular expenditure or non-compliance with laws and regulations.

## Whole of Government Accounts

The current deadline for completion of the Whole of Government Accounts (WGA) is 12 August 2013. However, there are currently a number of delays in HM Treasury rolling out the new data capture tool and providing guidance on the WGA process for 2012-13. The Group fall below the de-minimus threshold for audit of the WGA.

### 3. Financial Position

The key source of funding for the Council is the Scottish Government. In 2012-13, the Council received grant-in-aid totalling £49.3m, an increase of £10.9m (28%) from 2011-12. The Council has a general reserve balance of £9.0m at 31 March 2013.

The Lottery Fund's key source of income is from the National Lottery Distribution Fund. In 2012-13 the Lottery Fund received £31m, an increase of £6.1m (24%) from 2011-12. General reserve balance of £39.8m at the 31 March 2013.

#### Income

In 2012-13, the Council received £49.3m from the Scottish Government, an increase of 28% from 2011-12. £42.65m of this was in relation to grant-in-aid, while the other £6.65m was from other Scottish Government Grants, primarily Physical Activity (£1.2m) and Cashback for Communities Fund (£4.9m).

Income of £5.6m received by the Council is primarily for activities carried out by the Trust (£4.3m). This includes course fees (£2.1m), hires, sales and hospitality (£1.2m) and donations (£0.9m). There has been an increase of £0.75m (16%) in income from activities which can be attributed to the donation. Other operating income (£1.1m) has reduced by £0.18m. There was a reduction in high performance income of £0.19m.

The Lottery Fund received £31.1m in income, which £31m, was from the National Lottery Fund proceeds. This was an increase of 24% compared to 2011-12. During the year £27.4m was drawn down from the National Lottery Distribution Fund towards the payment of approved awards and the administration of the Lottery Fund.

Figure 1 – Total funding in 2012-13 compared to 2011-12

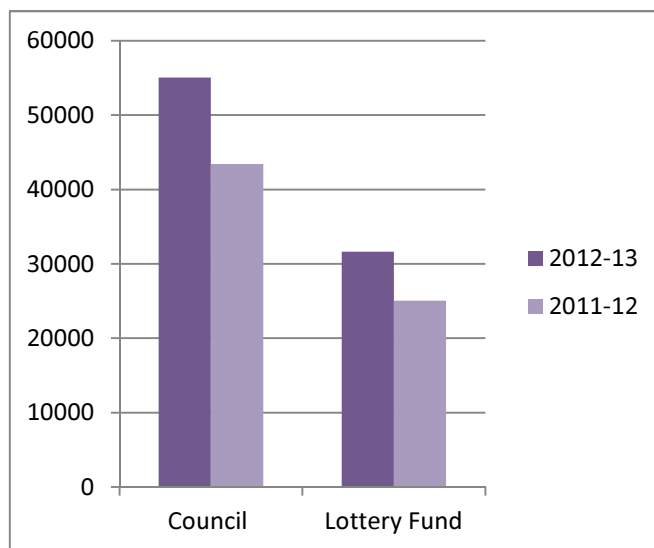
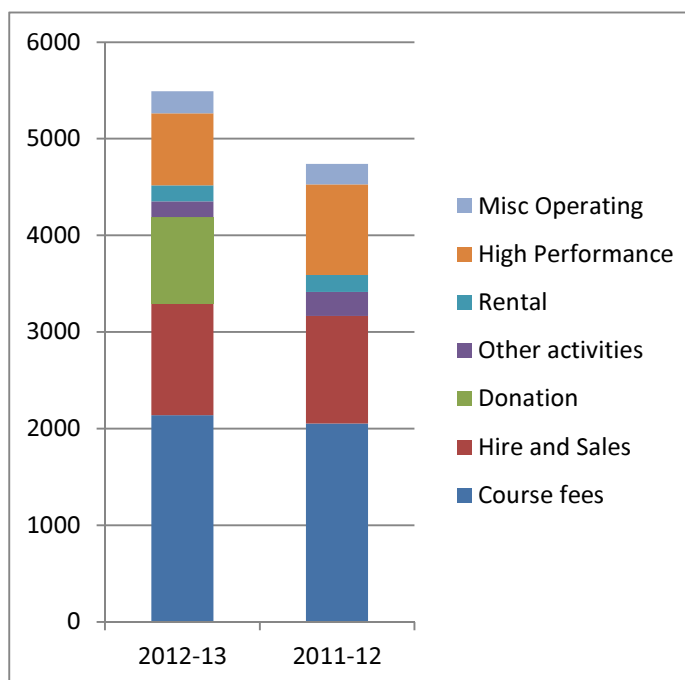


Figure 2 – key elements of Council income





## Grant Payments

Figure 3 shows the movement in total grants paid for the Council and the Lottery Fund from 2011-12 to 2012-13. The Lottery Fund shows a decrease in grants paid and net grant commitments for 2012-13 compared to 2011-12 by £7m (25%). This is due to fewer grants paid and committed in the year as net commitments made remained consistent over the two year period. Despite the increase in funding, the fall in grants is in line with the Corporate plan for 2011-15.

Figure 3 - Total Grants Paid (and net grant commitments for Lottery Fund)



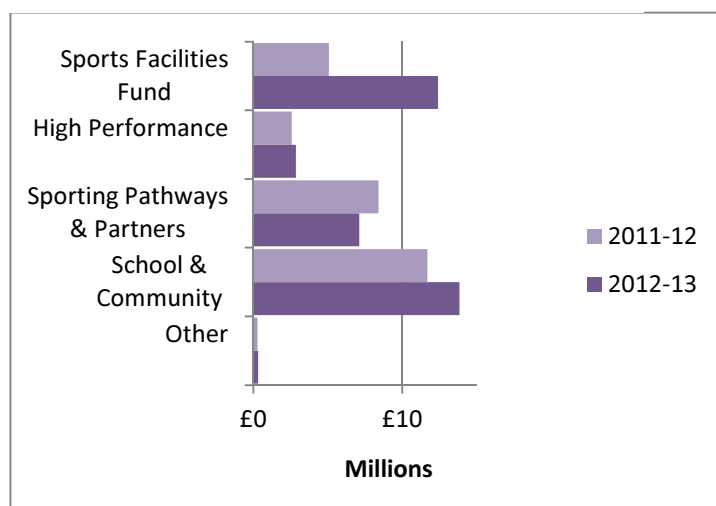
During 2012-13, the Council paid out revenue and capital grants of £36.5m, an increase of 30% on 2011-12. Over 70% of grants paid by the Council in 2012-13 were to Schools & Community (38%) and the Sports Facilities Fund (34%).

Schools & Community grants paid out increased by 18% from £11.6m to £13.8m in 2012-13. This has allowed significant progress to be made across the key programmes within school sport, with over 4.4m participants in the flagship programme Active Schools.

The Sports Facilities Fund share of total grants paid out increased by 16% during 2012-13, with grants paid out

increasing from £5.07m to £12.4m. This was due to the additional £7.5m being received from the Scottish Government during the year specifically to spend in this area.

Figure 4- Split of grants paid by the Council



## Other expenditure

Table 1 shows the split of other expenditure (excluding expenditure in relation to grants):

**Table 1 – movement in other expenditure (excluding grants)**

	2012-13	2011-12	Movement
	£'000	£'000	
Council	16,142	15,479	4.2%
Lottery Fund	5,627	4,636	21%
<b>Total</b>	<b>21, 769</b>	<b>20,115</b>	<b>8%</b>

The total monetary movement is an increase of £1.65m over the year. This is as a result of an increase in administration expenditure in both the Council and Lottery Fund (noted in Other operating charges per the annual accounts). This expenditure is related to general administration costs carried out by sportscotland to implement the grants being paid out. Due to increases in funding received from the Scottish Government and the correlated increase in grants paid, there was an expectation that this would increase in the year.

## Financial Position

The Council's statement of financial position reflects a positive financial position with general reserves of £9.0m (per Table 3), with total net assets being £6.2m (as noted in Table 2).

Non-current assets increased due to reallocation of £0.3 million from investment property, £1.2m of capital additions in the Trust, off set in the year with £0.2m of disposals, and £0.8m of depreciation.

Statement of Financial Position	2013	2012
	£'000	£'000
Non-current assets	12,423	11,906
Current assets	2,477	1,295
Current liabilities	(2,654)	(2,755)
Non-current liabilities	(6,032)	(3,555)
<b>Total net assets</b>	<b>6,214</b>	<b>6,891</b>

Within current assets, cash and cash equivalents increased by £0.6m in the year as did trade and other receivables. The increase in other trade and receivables is a result of the recognition of a donation received by the Trust which was not fully received at year end. The total amount of this donation was £0.9m with only £0.5m being received at the 31 March 2013.

Non-current liabilities increased by 69% (£1.9m) as a result of the increase in the Strathclyde Pension Fund liability at the 31 March 2013, which is also noted in table 3.

**Table 3 – Tax Payers Equity (the Council)**

Tax Payers Equity	2013	2012
	£'000	£'000
General fund (excluding pension reserve)	9,046	8,342
Revaluation Reserve	1,927	2,027
Other Reserves	1,198	-
Pension Reserve	(5,957)	(3,478)
<b>Total</b>	<b>6,214</b>	<b>6,891</b>

**Table 2 - Statement of Financial Position (the Council)**

The Lottery Fund's statement of financial position reflects a positive financial position with general reserves of £39.8m.

An increase in cash at bank of £2m is a contributory factor in the overall increase in current assets. In addition, investments from the National Lottery Distribution Fund increased by £1.9m.

Non-current liabilities within the Lottery Fund is in relation to grant commitments payable within 2 to 5 years, and has fallen due to a reduction in longer term commitments made in 2012-13.

**Table 4 - Statement of Financial Position (the Lottery Fund)**

Statement of Financial Position	2013 £'000	2012 £'000
Non-current assets	34	29
Current assets	53,008	49,953
Current liabilities	(12,450)	(12,635)
Non-current liabilities	(1,503)	(2,016)
<b>Total net assets</b>	<b>39,881</b>	<b>35,331</b>

### Looking forward

The Business Plan for 2013-15 indicates a 15% increase in budget between 2011-12 and 2013-14. This increase was mainly between 2011-12 and 2012-13, where £7.5m was received for the Sports Facilities Fund for a one off allocation for facilities investments, and £2.5m for Cashback which was part of a three year programme which is nearing its conclusion.

While these sources of funding are unlikely to be available during 2013-14, the higher level of investment is being sustained during the coming year by increases in the use of the National Lottery Funding for Club Sport and the additional Scottish Government Funding for Performance Sport.

The Council and Lottery Fund budget summary for 2013-14 estimates funding and income of £74.3m. 57% of this is estimated to come from the Scottish Government, of which £34.1m will be Grant-in-aid. 39% is estimated from the National Lottery with other income from Caledonia House (£0.2m) and UK Sport Income (£0.7m).

Within their planned expenditure for 2013-14, the Council and Lottery Fund have allocated on a programme by programme basis. Of the £64.6m programme budget, expenditure is expected to be split to the following programmes:

**Table 5- planned programme expenditure 2013-14**

Planned Expenditure	2013-14
School Sport	23%
Club Sport	15%
Performance Sport	22%
People	4%
Places	24%
Partnership and Planning	7%
Effective Organisation	5%

## 4. Governance

The Council has made improvements to the risk management arrangements which will need to be embedded in the organisation during 2013-14. The revised Trust Board arrangements have strengthened the governance of the Trust, a number of recommendations have been agreed which will further strengthen the arrangements.

### Annual Governance Statement

The Annual Governance Statement (AGS) is the key document that records the governance ethos of the Group, and assurances around the achievement of the vision and strategic objectives of the Council. The AGS summarises the governance structures in place, including the internal control framework, arrangements for risk management, financial governance and accountability.

### Risk Management

The Council has risk management arrangements in place. Risks are reviewed regularly by the Council and the Audit Committee. During the year, the Council have developed their approach to risk management. Progress has been made against a number of recommendations following an internal audit review of risk management. During 2013-14 the new arrangements will be rolled out and supported with a training programme.

### National Fraud Initiative

The Council have taken part in the National Fraud Initiative data matching exercise 2012/13. The Council have made good progress in reviewing the identified matches. To date there are no matches which have not been resolved.

### Scottish Sports Council Trust Company

Internal audit carried out a review of the governance arrangements in place for the Trust company.

Internal audit concluded that there is a generally sound system of control, with some elements of good practice. Six medium priority recommendations and one low priority recommendation have been made to improve arrangements for quality and consistency of reporting and board effectiveness.

During 2012-13 the Trust carried forward a deficit of £393k on general fund reserves. In addition, the Inverclyde premises has been deemed unfit for purpose. The Council need to assure themselves that the governance arrangements in place within the Trust are addressing the financial sustainability of the Trust company and that appropriate decisions are made in relation to the centre at Inverclyde.

## 5. Performance

The Council has a number of initiatives which have demonstrated Best Value. Considerable efforts continue to be made to identify core performance measures and how these relate to the outcomes.

### Corporate Plan

Guided by Scottish Government's policies, Let's Make Scotland More Active and Reaching Higher: Building on the success of sport 21, the Corporate Plan 2011-15 was launched in April 2011. The Corporate Plan outlines ten national outcomes and seven core functions. The delivery of these has been into six programme areas.

- Major progress is made in all key areas required for the development of a world class sporting system.
- 2011-15 is the most successful four year cycle for Scotland in terms of performance outcomes (London 2012, Sochi 2014 and Glasgow 2014).
- All supported performance athletes are the best ever prepared for all targeted events through the provision of quality services.
- An increasing number of Scottish Governing Bodies are fit for purpose and fit for performance.
- Major progress in growing sustainable levels of competent and skilled coaches, officials, administrators, specialists (paid and voluntary) within Scotland.
- A greater and more integrated role for outdoor and adventure sport, maximizing Scotland's unique attributes and heritage.
- Stronger club networks with greater community involvement.
- Increased sports opportunities for children and young people through schools and improved access to the school estate.
- Organisation development strengthens the impact of our work and we are driven by continuous quality improvement.

- **sportscotland** is seen as one of the leading public bodies in Scotland in terms of delivery, effectiveness and efficiency.

Progress with the implementation of the Corporate Plan is reported to the Council each quarter.

### Best Value

Accountable Officers have a specific responsibility to ensure that arrangements have been made to secure Best Value. In addition, the Boards (or equivalents) of relevant public service organisations have corporate responsibility for promoting the efficient and effective use of staff and other resources by the organisations in accordance with the principles of Best Value.

**sportscotland** has a number of initiatives in place to promote efficient and effective use of resources including:

- the development of Caledonia House as a House of Sport, providing accommodation and shared services to 18 organisations;
- provision of shared services for payroll services for a number of sports governing bodies;
- a procurement process which is delivering savings; and more effective cost management;
- investment in energy efficiency measures; and
- estates management.

### Performance reporting

**sportscotland** is developing its use of performance data. A selection of the current key performance indicators, which relate to the Council's outcomes are reported in the Annual Report and Accounts. The published indicators cover a range of information including

development of people, Active Schools and participation. Considerable efforts continue to be made, as new programmes are being developed to deliver the corporate plan, to identify core measures and how these relate to the outcomes described as the five changes in the Plan. This approach has been agreed as the basis for all quarterly reports to the Scottish Government and following a full presentation at its April 2013 meeting, it was endorsed by the **sportscotland** Board. The impact on the five changes is reviewed annually and at the end of the Corporate Plan period there will be an assessment of performance against the longer term measures set out in the Corporate Plan.

## National Studies

Audit Scotland carries out a national performance audit programme on behalf of the Accounts Commission and the Auditor General for Scotland.

Audit Scotland ask us to ensure that public sector bodies review the national studies relevant to them and action them accordingly. The Council has a protocol to summarise national reports for the Audit Committee or Board as appropriate.

During 2012-13, the Council executive considered the following reports and presented their findings to the Audit Committee and Board:

- Managing ICT Contracts – an audit of three public sector programmes
- Scotland's Public Finances – Addressing the challenges

## Managing ICT Contracts – an audit of three public sector programmes

The report, published in August 2012, reviewed three significant projects that were delayed, cancelled or overran on costs. The report identified that many of the problems stemmed from a lack of specialised information technology skills and experience. But there were also weaknesses in basic project management and control.

The key findings from the report included the need for:

- a business case supported by robust options appraisal

- clarity of roles and responsibilities within governance arrangements
- strong financial control, risk management and detailed progress reporting
- specialist skills and experience

**sportscotland** has a number of ICT projects including:

- replacement of facilities, SGB and Local Authority investment systems with Microsoft CRM
- replacement of document management system with Sharepoint
- development of the high performance athlete data management support system, Smartbase
- replacement bookings system at Glenmore lodge

Although much smaller than the case studies detailed in the Audit Scotland report, the same principals can be applied. The **sportscotland** report identified a number of practices **sportscotland** already conform to and improvements to the process which will be taken forward for future ICT projects.

## Scotland's public finances: Addressing the challenges

Scotland's public finances: Addressing the challenges was published by the Auditor General and the Accounts Commission in August 2011. The report provided an overview of the scale of budget cuts expected to be faced by the Scottish public sector in the period 2010/11 to 2014/15, and how public bodies were beginning to respond to the challenges of reducing expenditure.

As part of the programme of targeted follow up on national studies, Audit Scotland have requested that all relevant bodies are subject to targeted follow up work on Scotland's public finances: Addressing the challenges. We have reviewed how the Council is responding to the challenges of public sector budget constraints and the Council's efforts to achieve financial sustainability.

We specifically addressed the following questions:


- Does the Council have sustainable financial plans which reflect a strategic approach to cost reduction?
- Do senior officials and non-executive directors demonstrate ownership of financial plans and are they subject to sufficient scrutiny before approval?

Our overall conclusion is that whilst the Council has not faced the significant financial pressures and risks seen in other areas of the public sector, its current arrangements to secure efficiency and Best Value are satisfactory, with examples of good practice.


# Appendix A: IT General Control Recommendations

## Key to assessment of IT general control deficiencies


---

 Material weakness - risk of material misstatement

---

 Significant deficiency - risk of significant misstatement

---

 Deficiency - risk of inconsequential misstatement

---



	Assessment	Issue and risk	Recommendation
1	●	<p><b>Information technology – Developer access</b></p> <p>We noted that two Developers in the IT department could move changes to the live environment of the new CRM system. Both Developers could also create user accounts on this system.</p> <p>There is a risk that unauthorised changes are made to the CRM system.</p>	<p>We recommend that Developers are not granted access to the live environment of the CRM system to ensure adequate segregation of duties. If this is not possible due to staff constraints, the Council should implement a control to independently monitor all changes introduced to the live environment of the CRM system on a regular basis.</p> <p><b>Management response</b></p> <p>Developers now carry out work all development work for the CRM system in a separate development environment. Changes to the production environment are only implemented in the live environment once they have been tested and approved. Due to the nature of their role they will always require full access to the live environment for CRM, and this is something that <b>sportscotland</b> is satisfied with.</p>

	Assessment	Issue and risk	Recommendation
1	●	<p><b>Information technology – CRM implementation</b></p> <p>From our meeting with IT management and staff, we noted that several issues were experienced during the implementation of the new CRM system that resulted in delays. This implementation had just started its second phase at the time of our visit.</p> <p>There is a risk that issues that were present during the first phase of the CRM implementation are experienced again in subsequent phases of this project or when implementing any other systems in the Council.</p>	<p>The Council should hold a debrief meeting with members of staff to identify the lessons learned from the initial implementation of the CRM system. Once these lessons have been identified and documented, appropriate actions should be implemented to avoid these issues in the future.</p> <p><b>Management response</b></p> <p>In order to ensure a there is a comprehensive debrief and capture of “lessons learned” from all workstreams which comprise the project, this will take place by the end of September 2013 (Q2).</p>

	Assessment	Issue and risk	Recommendation
2	●	<p><b>Information technology - Leavers</b></p> <p>Human Resources (HR) or line manager report leavers to the IT department in order to get their access disabled. This communication is made through e-mail or verbally as there is not a standard leavers form. Additionally, HR sends a monthly email to IT detailing new starters and leavers in the past month. However, we understand that in some cases, leavers are not reported to the IT department prior to their leaving date.</p> <p>There is a risk that unauthorised access to data could be gained through the user account of a former member of staff or contractor.</p>	<p>The leavers process should be amended in the Council. HR or line managers should report leavers to the IT department prior to their leaving date. This communication should be made via a leavers form that could be electronic or in hard copy. Access for leavers should be disabled or removed on their leaving date.</p> <p>Additionally, the IT department should implement a monthly review process to disable network accounts that have not been used for a period of time (ie 90 days).</p> <p><b>Management response</b></p> <p>The existing HR policy states that the relevant line manager is responsible for completing the leaver’s form and advising all relevant people/teams of the individual leaving, including ICT. HR reminded line managers by e-mail on 8<sup>th</sup> May 2013 of this responsibility and reminding of the timescales for the disablement of network accounts.</p>

	Assessment	Issue and risk	Recommendation
3	●	<p><b>Information Technology – Change management</b></p> <p>We noted that there is no documented change management policy detailing the process to manage changes to IT systems or the IT infrastructure. However, we are aware that the Council intends to implement a change advisory board and patch management policy.</p> <p>There is risk that unauthorised or inappropriately tested changes are made to the IT environment. This could result in disruption to IT operations and have a detrimental impact on the Council reputation.</p>	<p>The Council should develop a policy to manage IT changes. This document should detail the change request forms that should be used to raise a change, approvals required, terms of reference for any change advisory board, testing procedure, sign offs for user acceptance testing and implementation processes.</p> <p><b>Management response:</b> A formal/documented change request process was implemented in early May 2013 for CRM developments. Due to the integrated nature and relatively small size of the ICT team and the open system architecture, we do not feel that a documented change control process for infrastructure operations is appropriate in terms of opportunity cost v's achievable benefits.</p>
4	●	<p><b>Information technology - User access reviews</b></p> <p>We understand that the IT department performs six-monthly reviews of network access rights but no evidence is retained of them. Additionally, no reviews are performed for the ITIS, CRM or Sage 500 systems.</p> <p>We noted that the following users have privileged access to the Council's systems without requiring it:</p> <p>Active directory (network)</p> <ul style="list-style-type: none"> <li>● a member of staff</li> <li>● a generic account</li> </ul>	<p>We recommend that the current process to review access rights at network level is formally documented. This review should also include applications like CRM, ITIS, Sage 500 and their database systems. The review should validate both the existence of users with access rights in these systems as well as the appropriateness of their access rights in relation to the users' job roles and responsibilities, with due consideration being given to adequate segregation of duties.</p> <p>Business management should be responsible for performing these reviews. IT staff should act as facilitators for providing the relevant information to management,</p>

	Assessment	Issue and risk	Recommendation
		<p>Dynamics CRM</p> <ul style="list-style-type: none"> <li>three members of staff have the system administration role</li> </ul> <p>ITIS (old investment system)</p> <ul style="list-style-type: none"> <li>three members of staff are designated as super users</li> </ul> <p>Sage 500</p> <ul style="list-style-type: none"> <li>An account had 'manager' status and it was not possible to identify the owner of this account.</li> </ul> <p>These users are listed in Appendix A.</p> <p>There is a risk that members of staff have access rights on the network or applications that are not commensurate with their current job duties. This could lead to unauthorised access to data.</p>	<p>collating the results and processing all amendments requested by management. Evidence of these reviews should be retained.</p> <p>Additionally, the Council should revalidate privileged user access at network, database and application levels on a quarterly basis. Privileged access for the users listed in Appendix A should be revised.</p> <p><b>Management response</b></p> <p>We will work with the relevant business departments to develop regular documented reviews of access rights to the network and key systems with the aim of having a formal process in place by end September 2013.</p> <p>With regard to the users highlighted with current access:</p> <p>Active directory – we are reviewing the 2 user accounts, one of which is for our SharePoint administrator, with a view to removing from the Domain Admin group</p> <p>Dynamics – these accounts had been given rights to assist with minor changes and testing. These have now been removed</p> <p>ITIS – These three users have appropriate permissions for their roles and have been left in place.</p> <p>Sage 500 – issue resolved (Head of Finance).</p>

	Assessment	Issue and risk	Recommendation
5	●	<p><b>Information technology – Password settings</b></p> <p>We noted the following password settings at network level</p> <ul style="list-style-type: none"> <li>• passwords are forced to be changed every 180 days. However, two user accounts, who belong to members of staff and have privileged access to the network and CRM systems, were noted to have passwords that never expire. We understand that there is no technical justification for the existence of this setting.</li> <li>• minimum password length is 5 characters</li> <li>• complexity is not enabled</li> <li>• password history is not enabled</li> </ul> <p>Additionally, network accounts are locked out for 1 minute after 30 invalid logon attempts.</p> <p>The Sage application requires a user ID and password to log on. However, we understand that none of the password parameters detailed above are configured.</p> <p>There is a single sign-on facility at the Council and users can access the new CRM application once they have logged onto the network. Therefore, there is a risk that unauthorised access could be gained to the network or CRM application through password guessing.</p>	<p>We recommend that passwords at network level are ruled by the following parameters as per the Council's new password policy:</p> <ul style="list-style-type: none"> <li>• passwords are forced to be changed every 90 days</li> <li>• minimum password length is 8 characters</li> <li>• passwords are forced to be complex</li> <li>• the last four passwords could not be reused</li> </ul> <p>Network accounts should be locked out for a longer period of time (ie 30 minutes) after a fewer number (ie 3 attempts) of invalid logon attempts.</p> <p>All network accounts should have passwords that expire in line with the policy aforementioned.</p> <p>We also recommend that the new password policy is implemented in the Sage 500 application. If this application does not allow these settings to be configured, the Council should ask users to manually set and change passwords in line with the policy.</p> <p><b>Management response</b></p> <p>A new password policy has been developed and agreed by the SMT for implementation by end June 2013. This encapsulates the recommended changes above. The ICT team will explore with the Finance Team the possibility of enabling similar policies in Sage Line 500, dependant on available options within the system. Review to be completed by end June 2013.</p>

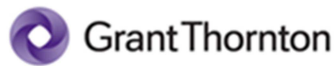
	Assessment	Issue and risk	Recommendation
6	●	<p><b>Information technology – Vulnerability assessment</b></p> <p>No vulnerability assessment or penetration test has been performed, although, we understand that the Council intends to perform one later this year once a specific software is implemented.</p> <p>By not performing a vulnerability assessment, there is a risk that vulnerabilities in the IT security infrastructure of the Council are exploited resulting in disruption to IT operations or unauthorised access to data.</p>	<p>We recommend that vulnerability assessments are performed at least on an annual basis for the Council's IT infrastructure. Any vulnerabilities identified should be promptly addressed.</p> <p><b>Management response</b></p> <p>An annual schedule of testing has been developed to check these vulnerabilities, ensuring results are documented, and any recommendations are addressed appropriately. The first test will take place during October 2013.</p>
7	●	<p><b>Information technology - Audit logging</b></p> <p>The Windows network has various audit logs where security events are recorded. These logs detail when a user logged on to the network or the date on which, access rights to the domain were changed. From our enquiries, we understand that such audit logs are not validated on a regular basis due to the overhead on the servers that their recording would entail.</p> <p>By not checking the network audit logs on a regular basis, there is a risk that unauthorised activity on the network (such as a user trying to guess the password of someone's else account), might go undetected. This could lead to unauthorised access to data stored on the network.</p>	<p>A process to review the network security log on a regular basis should be implemented. This process should involve the definition of the events to be monitored (i.e. failed logon attempts or changes to user access rights) and the frequency for this review. Any unusual activity on the network should be investigated and documented.</p> <p>The Council may consider using an off-the-shelf software tool to review the network audit logs. This could increase the efficiency and effectiveness of this review.</p> <p><b>Management response</b></p> <p>This has been explored and due to the significant overheads and staff time that auditing of this nature would incur it is viewed appropriate to continue with current arrangements, which includes monitoring of network activity and investigation of unusual events.</p>

	Assessment	Issue and risk	Recommendation
8	●	<p><b>Information technology - Memory sticks</b></p> <p>We understand that data could be written to unencrypted memory sticks in the Council. However, we understand that IT Management were intending to implement software to restrict this issue once an IT replacement project were completed later this year.</p> <p>If a memory stick with personal or sensitive data were lost, there is a risk that it may expose the Council to negative publicity, lead to fines imposed by the Information Commissioner's Office or unauthorised access to data.</p>	<p>Write access should only be allowed to encrypted memory sticks. Staff should not be able to copy data to unencrypted memory sticks unless there is a valid business reason for it and it has been duly authorised.</p> <p>Members of staff should be reminded about the appropriate use of personal storage devices such as memory sticks and the risks that their use entails.</p> <p><b>Management response</b></p> <p>A DLP solution (McAfee) has been identified and will be fully implemented by end September 2013. This will lock down all USB ports to permit access only to authorised USB devices. An assessment will be undertaken throughout the roll-out to ensure that any restrictions are not prohibitive to staff in their day to day work and alternative solutions identified.</p>



	Assessment	Issue and risk	Recommendation
9	●	<p><b>Information technology – Disaster recovery</b></p> <p>We understand that the Council performs regular recovery tests of IT systems by using the alternate server room in Edinburgh. However, these tests are not documented.</p> <p>Additionally, full backups are generated to tape on a daily basis but they are kept in safe at the Glasgow server room.</p> <p>There is a risk that the recovery of IT systems could take longer than the Council could accommodate and this could result in reputational damage.</p>	<p>We recommend that disaster recovery tests are documented and analysed to identify any relevant improvements to the IT recovery arrangements.</p> <p>Backup tapes should be sent to an alternate location on a regular basis. This location should have adequate environmental and security conditions for the storage of backup media.</p> <p><b>Management response</b></p> <p>Documented testing in line with the DR policy commenced in early May 2013 with a Primary Internet Connection Failure Test – which worked as required. A comprehensive test schedule will be repeated annually thereafter, with results captured and documented.</p>

	Assessment	Issue and risk	Recommendation
10	●	<p><b>Information technology – IT policy</b></p> <p>There is a computer user and information toolkit policy within the Council. Members of staff do not formally confirm their understanding and compliance with this policy. However, Human Resources is in the process of implementing a system so members of staff would be able to provide this confirmation electronically.</p> <p>There is a risk that the Council could not be able to hold members of staff accountable for a misuse of IT resources.</p>	<p>We recommend that the process to implement the electronic confirmation of the computer user and information toolkit policy is completed at the earliest convenience. Once active, all members of staff should be asked to complete this confirmation.</p> <p><b>Management response</b> This is now captured within the e-learning process which is scheduled to be implemented on a rolling programme from May 2013. The timescale for the information and computer user toolkit has been brought forward to September 2013 and during the intervening period the toolkit will be reviewed and updated by the Information Asset Manager.</p>
11	●	<p><b>Information technology – User request form</b></p> <p>The ICT user request form does not consider the new CRM system. This form is sent to the IT department to request the creation of new user accounts.</p> <p>There is a risk that users are granted inappropriate access rights in the new CRM system.</p>	<p>We recommend that the ICT user request form is amended to reflect the new CRM system. This form should list the available CRM roles that could be granted to members of staff.</p> <p><b>Management response</b> The form will be amended for use from June 2013 (following discussion with HR).</p>



© 2013 Grant Thornton UK LLP. All rights reserved.

'Grant Thornton' means Grant Thornton UK LLP, a limited liability partnership.

Grant Thornton UK LLP is a member firm within Grant Thornton International Ltd ('Grant Thornton International').

Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered by the member firms independently.

This publication has been prepared only as a guide.

No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication

[www.grant-thornton.co.uk](http://www.grant-thornton.co.uk)