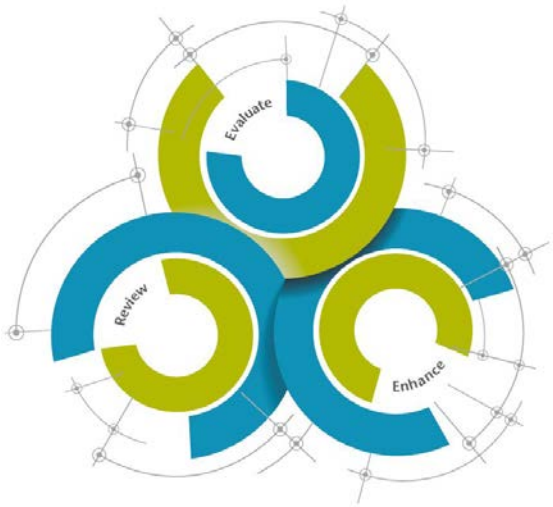
Chartered Institute of Internal Auditors



EXTERNAL QUALITY ASSESSMENT (EQA) REPORT FOR

Scottish Enterprise

Prepared by Chris Baker and Pauline Scott on behalf of

The Chartered Institute of Internal Auditors,

15th November 2016

Chartered Institute of Internal Auditors

TABLE OF CONTENTS

Opinion, including level of conformance to the International Professional Practices Framework (IPPF)

Scottish Enterprise (SE) has an effective internal audit (IA) service. It is held in high regard for its integrity, honesty, challenge and practical advice founded upon independence and objectivity (further stakeholder feedback is available in appendix 1). SE internal audit is in the upper quartile of all the IA functions we have reviewed (approximately 80 functions since 2012) making it one of the better IA operations we have seen.

The Institute of Internal Audit's (IIA's) International Professional Practice Framework (IPPF) includes the Definition of Internal Auditing, Code of Ethics, and the *International Standards*. There are 56 fundamental principles to achieve with more than 150 points of recommended practice. Below is a summary of how the SE internal audit function performs to the IPPF.

Summary of IIA Conformance	Standards	Does not Conform	Partially Conforms	Generally Conforms	Total
Definition of IA and Code of Ethics	Rules of conduct			5	5
Purpose	1000 – 1130			7	7
People	1200 – 1230			4	4
Performance	1300 – 1322			7	7
Planning	2000 – 2130		1	11	12
Process	2200 – 2600		2	19	21
Total			**3**	**53***	**56**

This is an excellent result given the breadth of the IPPF and with progress on our recommendations IA can say it "generally conforms to the IIA standards".

The recommendations in the table below reflect the achievements of the organisation and internal audit but also the opportunities available (an overview is set out in the SWOT analysis at appendix 2). As such we offer a group of recommendations related to risk management that work towards maintaining robust corporate governance. These recommendations will stretch IA and will require the continued direction of the Audit Committee and support of senior management, nevertheless we feel they are achievable and will deliver best practice through continued collaboration and teamwork. These opportunities are also reflected in the IA Maturity matrix at appendix 3 and will help to monitor progress.

(*There are 5 specific standards that mainly relate to reporting and using the term conformance to the Standards that are currently not applicable to SE)

Recommendations to further enhance the effectiveness of Internal Audit

Coordination of assurance (Standard 2050 partial conformance)	Response & action date
An opportunity exists as part of the ongoing development of risk management to extend the corporate risk register to formally identify those internal and external assurance providers who verify that risk mitigation action and controls are working. Assurance Maps have the potential to: • Illustrate the linkage between risks, controls and audit creating a 3 lines of defence model. • Identify the full scope of assurance activity, both internal and external, to enable further coordination. • Give visibility to any duplication or gaps in assurance activity to gain maximum coverage for the audit committee. • Enable internal audit to review and place reliance upon other assurance providers where appropriate adding further value to available internal audit time. • Give more breadth to the assurance coverage to support the audit committee's annual governance statement. • Raise the overall profile of the risk management process. **We therefore recommend the creation of a simple but effective Assurance Map, identifying who provides assurance for each of the management actions/key controls in the strategic risk register as a basis for enhanced coordination. This will enable internal audit to state how it intends to use other sources of assurance and articulate any work required to place reliance upon those other sources (as required by the PSIAS).**	Agreed. An Assurance Map will be developed and presented to the Audit Committee for approval. March 2017.
Planning (Standard 2010)	**Response & action date**
Standard 2010 relates to "establishing risk based audit plans to determine the priorities of internal audit activity." We have seen good evidence of how elements of the SE internal audit plan aligns to corporate risks.	

From this base there is scope to simplify the presentation of this risk based plan while making it more informative to the audit committee. **This can be achieved by providing a simple narrative that links specific corporate risks, to management responses (controls & monitoring) and the primary focus of individual audits. This will add further rationale to the selection of audits and give transparency to any risk excluded or deferred enabling informed discussions about what is audited, why and the overall resource level needed.** (We have provided a number of examples of assurance maps and audit plans, some of which are combined to provide ideas and options)	Agreed. This recommendation will be implemented within the 2017/18 Internal Audit Plan. The Plan will be presented to the Audit Committee for approval. March 2017.
Engagement scope (Standard 2220 partial conformance)	**Response & action date**
Development of an assurance map and the audit plan will also enable most of the terms of reference of individual audits to be explicitly focused upon risk. IA are ideally positioned to review both the application of risk processes and the mitigation of risks in almost every audit they do. **We therefore recommend the scope of audits be expanded to enhance the risk based approach. In addition the trust that IA has earned will enable to explore and report upon the root causes of issues, some of which may be cultural and we would encourage this approach in appropriate situations to provide leading internal audit practice.** (We have passed on IIA guidance on how such techniques can be approached)	Agreed. The scope of audits will be enhanced in line with the revised approach to planning and assurance (see above). In addition, the scoping document will be updated to better reflect a risk based approach. March 2017.
Policies and procedures (Standard 2040)	
The current IA methodology is an effective one and is applied consistently with due supervision and coaching. However, there is good deal of administration in the process creating the potential for some streamlining and increased efficiency. **While the existing methodology could be made leaner we also believe it is worth considering the purchase of both audit management software (particularly one that has a risk management module) and/or audit data analysis tools. Such systems are particularly suited to dispersed teams and cater for expansion.**	Agreed. The options for audit management software and/or audit data analysis tools will be fully considered. March 2017.

Communicating the Acceptance of Risk (Standard 2600)	Response & action date
The standards guide internal auditors to draw attention to weaknesses, inadequacies and/or failures in control and the value of relating this back to risk scoring and risk appetite. For example residual risk scores may need to be higher with the organisation accepting a higher level of risk as a result of poorly performing controls, as identified during an audit. **IA is positioned well to implement this standard once discussions on risk appetite give more clarity to risk tolerances and we recommend that it would beneficial for auditors to draw attention to the impact of poorly performing or inadequate controls on residual risk scores within their reports.**	Agreed. Will be implemented for 2017/18 audits within the 2017/18 Internal Audit Plan. June 2017.
Overall Opinion (Standard 2450 partial conformance)	**Response & action date**
IA meet the public sector requirement to prepare an annual report and opinion. However, we feel IA can give a stronger governance message by providing more commentary upon the overall effectiveness of risk management. **Through its work IA has a unique perspective on risk management and we would encourage and recommend IA to express their view upon the developing maturity of risk management in the organisation, the application of risk processes and the overall mitigation of risks.**	Agreed. Following the implementation of the recommendations in this EQA report, the overall opinion will be updated accordingly. March 2018.
Internal Audit Charter (Standard 1000)	**Response & action date**
The current IA Charter fully conforms to the Standards containing all the required elements but it does not do justice to the full range of services and priorities of the team. **To provide a Charter that is specifically tailored to the needs of SE and the recommendations we have offered. As such we suggest the Charter could be briefly expanded in due course to articulate how the risk audit plan is to be formulated to provide a broad annual opinion, including IA's specific approach to providing assurance in relation to the key areas of governance, risk management and projects.**	Agreed. The Internal Audit Charter will be updated. March 2017.

Other items for consideration	Response & action date
• Possible break down of large 60 day audits into subsections around specific risks with interim reports and/or the introduction of smaller 'key control' audits. • Preparation of a forward plan for future quality assessment agreed with audit committee we suggest a plan that works back from the next EQA. • Affiliate membership to the CIIA to support development of the team.	Agreed. To be implemented as part of the 2017/18 Internal Audit Plan. March 2017. Agreed. A forward plan for future quality assessment will be presented to the Audit Committee for approval. March 2017. Agreed. Affiliate membership to be progressed. March 2017.

Stakeholder feedback

Appendix 1

We use the IIA's 10 Core Principles that define effective internal audit to structure discussions with stakeholders.

As the results opposite show IA scores high against all of these core principles with trusted advisor, honest broker and independent assurer scoring particularly impressively.

These attributes and others came through strongly and consistently in all of the interviews and is testament to the leadership of the team.

At the same time there is a strong desire among stakeholders for these standards to be maintained and to be built upon. High on the agenda is the need for IA to retain and develop its talent to provide succession and potential growth. In addition there is a desire that IA should continue to be a key influencer and change leader within the developing risk culture.

Interviewees	Title/Position
Willie Mackie	SE Board and Audit Committee chair
Grahame Smith	SE Board and Audit Committee member
Alison McGregor	SE Board and Audit Committee member
Melfort Campbell	SE Board and Audit Committee member
Lena Wilson	Chief Executive
Iain Scott	Chief Financial Officer
Jim McRoberts	Risk Manager
Carolyn Stewart	Managing Director People
Liz Maconachie	Audit Scotland
IA Team members – Alan Browne, Mark Donohoe, Jennifer Paul, Allan Johnston	

Chartered Institute of Internal Auditors

SWOT Analysis **Appendix 2**

What works well (Strengths)	What could be done better (Weaknesses) (This cover the Non and Partial Comformances)
• IA has a high profile and status within SE. • Strong and respected leadership. • IA is independent and trusted to make robust challenge. • Strong relationships with the Board (AC) and management at all levels. • Experienced and qualified team with understanding of SE and the sector. • Use of outsourced resource for audit of specialist areas. • Defined and consistent use of the audit methodology. • Embedded process for the follow up of audit recommendations. The low level of outstanding audit recommendations demonstrates robustness. • Focus on CPD and team development e.g. training opportunities. • Succession planning.	• Reducing the wordiness in audit documentation and reports. • Use of computer assisted audit techniques to enable more depth of sampling and analysis. • Greater clarity in defining IA's role in relation to risk management and projects. • Closer links with the profession to maintain best practice.
What could deliver further value (Opportunities)	**What could stand in your way (Threats)**
• Assurance mapping for key risks which incorporates all assurance providers – using the assurance map to review assurance need and resources. • Greater co-ordination with other internal assurance providers especially in relation to coverage of key risks. • Joint working and greater synergy with second line of defence teams. • Developing the narrative within the audit plan to show the link between risks, management responses and audit priorities. • More flexible and dynamic audit planning to respond to emerging risks. • Auditing against criteria of success and risk appetite. • Encouraging auditors to use root cause analysis. • Shorter "Light touch" audit methodology for previous audit areas and key control audits. • Streamlining the audit process with reporting format. • A more robust risk management annual opinion. • Potential expansion and growth of the service to other clients.	• Reliance upon key members of staff. • Lack of opportunities for promotion and new challenges within the team to enable retention. • Ever expanding knowledge and skills required of the team. • Financial constraints.

Chartered Institute of Internal Auditors

Internal Audit Maturity

Appendix 3

Assessment	IIA standards	Focus on performance, risk and adding value.	Coordination and maximising assurance	Operating with efficiency	Quality Assurance and Improvement Programme
Excellent	Outstanding reflection of the IIA standards, in terms of logic, flow and spirit. Generally conforms in all areas.	IA alignment to the organisation's objectives, risks and change. IA has a high profile, is listened to and is respected for its assessment, advice and insight.	IA is fully independent and is recognised by all as a 3rd line of defence. The work of assurance providers is coordinated with IA reviewing reliability of.	Assignments are project managed to time and budget using tools/techniques for delivery. IA reports are clear, concise and produced promptly.	Ongoing efforts by IA team to enhance quality through continuous improvement. QA&IP plan is shared with and approved by AC.
Good	The IIA Standards are fully integrated into the methodology – mainly generally conforms.	Clear links between IA engagement objectives to risks and critical success factors with some acknowledgement of the value added dimension.	Coordination is planned at a high level around key risks. IA has established formal relationships with regular review of reliability.	Audit engagement are controlled and reviewed while in progress. Reporting is refined regularly linking opinions to key risks.	Quality is regarded highly, includes lessons learnt, scorecard measures and customer feedback with results shared with AC
Satisfactory	Most of the IIA Standards are found in the methodology with scope to increase conformance from partially to generally conform in some areas.	Methodology requires the purpose of IA engagements to be linked to objectives and risks. IA provides advice and is involved in change but criteria and role require clarity.	The 3 lines of defence is model is regarded as important. Planning of coordination is active and IA has developed better working relationships with some review of reliability.	Methodology recognises the need to manage engagement efficiency and timeliness but further consistency is needed. Reports are informative and valued.	Clear evidence of timely QA in assignments with learning points and coaching. Customer feedback is evident. Wider QA&IP may need formalising
Needs improvement	Gaps in the methodology with a combination of non-conformances and partial conformances to the IIA Standards.	Some connections to the organisation's objectives and risks but IA engagements are mainly cyclical and prone to change at management request.	The need to coordinate assurance is recognised but progress is slow. Some informal coordination occurs but reviewing reliability may be resisted.	Multiple guides that are slightly out of date and form a consistent and coherent whole. Engagement go beyond deadline and a number are deferred	QC not consistently embedded across the function. QA is limited / late or does not address root causes
Poor	No reference to the IIA Standards with significant levels of non-conformance.	No relationship between IA engagements and the organisation's objectives, risks and performance. Many audits are adhoc.	IA performs its role in an isolated way. There is a feeling of audit overload with confusion about what various auditors do.	Lack of a defined methodology with inconsistent results. Reports are usually late with little perceived value.	No evidence of ownership of quality by the IA team.

IIA Grading Definitions **Appendix 4**

The following rating scale has been used in this report.

Overall Audit Grading	
Generally Conforms (GC)	The assessor has concluded that the relevant structures, policies, and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual Standard or element of the Code of Ethics in all material respects. For the sections and major categories, this means that there is general conformance to a majority of the individual Standards or elements of the Code of Ethics, and at least partial conformance to the others, within the section/category. There may be significant opportunities for improvement, but these must not represent situations where the activity has not implemented the Standards or the Code of Ethics, has not applied them effectively, or has not achieved their stated objectives. As indicated above, general conformance does not require complete/perfect conformance, the ideal situation, successful practice, etc.
Partially Conforms (PC)	The assessor has concluded that the activity is making good-faith efforts to comply with the requirements of the individual Standard or element of the Code of Ethics, section, or major category, but falls short of achieving some major objectives. These will usually represent significant opportunities for improvement in effectively applying the Standards or Code of Ethics and/or achieving their objectives. Some deficiencies may be beyond the control of the activity and may result in recommendations to senior management or the board of the organisation.
Does Not Conform (DNC)	The assessor has concluded that the activity is not aware of, is not making good-faith efforts to comply with, or is failing to achieve many/all of the objectives of the individual Standard or element of the Code of Ethics, section, or major category. These deficiencies will usually have a significant negative impact on the activity's effectiveness and its potential to add value to the organisation. They may also represent significant opportunities for improvement, including actions by senior management or the board.

Often, the most difficult evaluation is the distinction between general and partial. It is a judgement call keeping in mind the definition of general conformance above. The assessor must determine if basic conformance exists. The existence of opportunities for improvement, better alternatives, or other successful practices does not reduce a "generally conforms" rating.