SSSC

Risk Management

Internal Audit Report No: 2021/02

Draft issued:	**9 July 2020**
2nd Draft issued:	**10 July 2020**
3rd Draft issued:	**10 July 2020**
Final issued:	**17 July 2020**

LEVEL OF ASSURANCE	**Good**

Now, for tomorrow

mha HENDERSON LOGGIE

Contents

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the organisation to material risk and which requires to be brought to the attention of management and the Audit and Assurance Committee.
Priority 2	Issue subjecting the organisation to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

Management Summary

Overall Level of Assurance

Good	System meets control objectives

Risk Assessment

This review focused on overarching risk management arrangements within the SSSC and therefore the review encompasses all identified risks facing the organisation rather than any specific risk or risks.

Background

As part of the Internal Audit programme at the SSSC for 2020/21 we carried out a review of the risk management arrangements across the organisation. This was identified by the Executive Management Team as an area where risk can arise and where Internal Audit can assist in providing assurances to the Council and the Chief Executive that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level. This position was endorsed by the April 2020 meeting of the Audit and Assurance Committee.

As a Non-Departmental Public Body, the SSSC is subject to the requirements of the Scottish Public Finance Manual (the SPFM). The SPFM contains specific guidance on risk management arrangements and specifies the following as highlights key point that should be considered when developing your organisation's risk approach:

- **Tied to Objectives:** Risk Management needs to be tied to your purpose and your objectives essentially what you are trying to achieve. If you aren't clear what your aims are then you can identify your risks effectively.
- **Systematically approached:** There is no single right way to identify and record an organisation's risk profile but taking a systematic approach to identifying risks and maintaining a clear record is critical to effective risk management.
- **Clearly described:** Risks should be prioritised in relation to objectives. A risk description should be a combination of both the possible cause and the possible impact to your objective.
- **Responsibly owned:** All risks, once identified, should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored appropriately.

Background (Continued)

- **Supported by a defined framework**: It is important to develop a framework for assessing risks which evaluates both the likelihood of the risk being realised, and of the impact if the risk is realised. Risk assessment should be recorded in a way that clearly demonstrates the key stages of the process.
- **Identified risk appetites:** Determining your "risk appetite" is key to achieving effective risk management and is essential to support decision making and supports how risks can ultimately be addressed.
- **Regularly Monitored:** The management of risk should be reviewed regularly to monitor whether or not the risk profile is changing, to gain assurance that risk management is effective, and to identify when further action is necessary.
- **Effectively communicated:** Raising awareness about potential problems and sharing important information can ensure better problem solving, provide effective challenge and support and support effective escalation.

Scope, Objectives and Overall Findings

The scope of this audit was to consider whether there were corporate policies and procedures in place to adequately assess risk and minimise the possibility of unexpected and unplanned situations developing.

The table below notes the objectives for this review and records the results:

Objective	Findings				Actions already underway
The specific objectives of this audit were to obtain reasonable assurance that:		**1**	**2**	**3**	
1. There is a process in place to provide reasonable assurance to Council and to the Chief Executive in relation to the declaration on risk required for the financial statements	**Good**	0	0	0	
2. The process in place applies good practice in risk management	**Satisfactory**	0	0	3	✓
3. Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and Council	**Good**	0	0	1	
Overall Level of Assurance	**Good**	**0**	**0**	**4**	
		System meets control objectives			

Audit Approach

We obtained and reviewed a copy of the SSSC risk management policies, procedures and Strategic Risk Register and discussed the risk management arrangements in place with the Director of Strategy and Improvement, as executive lead for risk management. We also held meetings with each of the other directors and their respective operational management teams (OMTs) in order to capture the experience of individual directorates in applying the risk management arrangements at directorate level. We also held a meeting with the managers responsible for overseeing the risk management process centrally within the Strategy and Performance directorate. The SSSC risk management arrangements were then benchmarked against relevant good practice guidance.

Summary of Main Findings

Strengths

- A comprehensive Risk Policy is in place which clearly articulates the SSSC approach to risk management and the responsibilities of the executive senior management team; the Audit and Assurance Committee and Council in identifying, assessing and monitoring the mitigation of risks.
- Updates on directorate risks are prepared as an integral part of the monthly Assurance Report submitted by each of the directorates to the Strategy and Performance directorate.
- The risk management element of the Assurance Reports submitted is sense checked by the central team before it is considered at the monthly Assurance Meetings.
- Risk management is a standing agenda item for each meeting of the Executive Management Team (EMT) and Operational Management Team (OMT) meetings within each directorate.
- The strategic risk register is maintained centrally within the Strategy and Performance directorate with an archive version maintained and a new version created each month which shows any changes made to the preceding version in tracked changes.
- The regular EMT discussions around risk allow ample opportunity for senior management discussion on the risks; the scoring of the risks; and the mitigating actions and controls in advance of each meeting of the Audit and Assurance Committee.
- From our attendance at the Audit and Assurance Committee meeting it was clear that there is a full discussion around risk management and a comprehensive presentation is provided with absolute transparency on key risks.

Opportunities for Improvement

- The current process for collating the monthly updates on the risk register is currently a time consuming and largely manual process.
- Our review of individual directorate risk registers highlighted some variation in the way in which risks are being described and in the way that associated risk actions and controls are being documented.
- We noted that although progress in delivering mitigating actions - on both the strategic and directorate risk registers - is closely monitored, there are currently no individual responsibilities and target implementation dates set for those actions which are not drawn from existing plans.
- Although risk appetite levels have been set for the risk categories these are not currently linked to the risk scoring matrix in a way which would allow identification of instances where residual risk is above the risk appetite level set by Council.

Acknowledgements

We would like to take this opportunity to thank the staff at SSSC who helped us during our audit.

Main Findings and Action Plan

Objective 1: There is a process in place to provide reasonable assurance to Council and to the Chief Executive in relation to the declaration on risk required for the financial statements

A comprehensive Risk Policy was approved by Council in March 2020 together with a risk appetite statement for the SSSC. We noted that a review date of December 2020 has been formally documented within the policy document. Good practice suggests that the adequacy of the risk management framework should be reviewed annually as part of the process to consider whether the Audit and Assurance Committee has delivered on the risk management element of the terms of reference. This is delivered through an annual member development event, hosted by the Audit and Assurance Committee, to review the Strategic Risk Register to which all Council Members and EMT are invited. The Risk Policy clearly states that "*This includes examination of the SSSC's track record on risk management and internal control*".

The Risk Policy sets out the standard risk management approach to be applied in relation to risk identification and review, as well as the subsequent monitoring of risks and mitigating management actions.

The Risk Policy clearly articulates the SSSC approach to risk management and the responsibilities of the EMT, the relevant directorate OMT, the Audit and Assurance Committee and Council in identifying, assessing and monitoring the mitigation of risks.

Updates on directorate risks are prepared as an integral part of the monthly Assurance Report submitted by each of the directorates to the Strategy and Performance directorate. The risk management element of the Assurance Reports submitted is sense checked by the central team before it is considered at the monthly Assurance Meetings. It is clear for our discussions with each of the directorates that this monthly reporting cycle has been embedded in a relatively short period of time and has been well received by the managers involved. Our meeting with the central team confirmed that directorates are producing the information requested and that this information is being produced in a timely fashion and in the required format. Risk management is a standing agenda item on the Executive Management Team (EMT) agenda as part of the Finance, Performance and Risk Report to EMT on a monthly basis. This allows discussion on any emerging directorate risks, highlighted within the monthly Assurance Reports, which may require to be escalated to the Strategic Risk Register or where further work may be required at corporate level to manage individual risks. The strategic risk register is maintained centrally within the Strategy and Performance directorate with an archive version maintained and a new version created each month which shows any changes made to the preceding version in tracked changes. The regular EMT discussions around risk allow ample opportunity for senior management discussion on the risks; the scoring of the risks; and the mitigating actions and controls in advance of each meeting of the Audit and Assurance Committee.

Risk Management

Objective 1: There is a process in place to provide reasonable assurance to Council and to the Chief Executive in relation to the declaration on risk required for the financial statements (continued)

Observation	Risks	Recommendation	Management Response	
Although there is clear engagement from all stakeholders the current process for collating the monthly updates on the directorate risk registers is a time consuming and largely manual process of reviewing each risk to ensure that updates have been provided; assessing these changes and then reflecting them on the face of the monthly update as part of the Assurance Report. There are software solutions available which would reduce the current administrative burden of collating the monthly updates and would allow the delivery of mitigating actions to be tracked more efficiently.	At peak work periods, the administrative burden of collating monthly updates may shift the focus away from the evaluation of proposed changes and supporting narrative to the physical collation of the update itself.	**R1** The possibility of procuring a risk management software solution should be explored with a business case developed which would evaluate the upfront and ongoing costs of the operating the software against the benefits which would accrue.	Agreed and we are currently looking to procure a risk and planning software package to be in place next year. **To be actioned by**: Director of Strategy & Performance **No later than:** 30 June 2021	
			Grade	**3**

Risk Management

Objective 2: The process in place applies good practice in risk management

We compared the risk management framework adopted by SSSC and compared this against the risk management guidance contained within the SPFM. Our evaluation of the evidence presented is summarised below against each of the headings included in the SPFM:

Tied to Objectives - the standard approach adopted ensures that the specific link between each risk and the SSSC Strategic Plan must be documented. However, we did not that several of the directorate risk registers reviewed did not have the outcome column populated. We also noted that work has already commenced to link mitigation and controls to established performance metrics so that performance outwith agreed parameters can be identified as a "risk trigger".

Systematically approached - the Risk Policy states that directorates will identify risks and document these using pro-forma documentation and the Risk Policy references the fact that a systematic process is in place to help identify risk and give assurance that there is a complete risk profile. The approach applied is identical for identifying and scoring both strategic and directorate risks, thereby ensuring consistency in approach. The approach to be adopted was explained to all directorates through several tailored sessions delivered in early 2020 by the Director of Strategy and Improvement. We noted that some directorates are operating a third tier of risk register with team risk registers developed which sit below the directorate level risk register. While this is not in place across all directorates, we are comfortable that this simply reflects the nature of the work of each directorate and the way in which the associated risks require to be managed.

Clearly described – Although the Risk Policy does set out the way in which directorates are expected to identify and document risks it is clear from our review of individual directorate risk registers that there is variation in the way in which risks are being described and in the way that associated risk actions and controls are being documented. Therefore, we would see merit in developing a procedure note which provides examples of the way in which risks should be articulated and demonstrates the way in which associated risk actions and controls should be documented in order to achieve further consistency in approach. This suggested enhancement to the existing arrangements is addressed in the action point noted below.

Responsibly owned - All risks on the strategic risk register are assigned to a single risk owner. This is always a member of EMT, although the responsibility for physically maintaining the associated controls or delivering the agreed management actions may rest with another manager depending on the nature of the risk. This risk owner is responsible for providing updates on each of the strategic risks as part of the monthly directorate reporting cycle described above.

Supported by a defined framework - There is a clear methodology for identifying and assessing both gross and residual risk scores. This includes risk descriptors which explains the meaning of each of the scores on the risk scoring matrix. Although mitigating actions, and comments on the progress made since the last review, are captured on the face of the strategic and directorate risk registers there are currently no target implementation dates set for mitigating actions. This is covered in more detail in a separate action point below.

Identified risk appetites - We noted that the current strategic risk register does not identify risks where the residual risk level exceeds the risk appetite set by Council. This is an area where further development is required to build on the existing arrangements. Again, this is covered in more detail below.

Regularly Monitored - As highlighted under Objective 1 above, there is regular reporting on risk management to EMT, the Audit and Assurance Committee and Council. The consideration of risk management is also built into the terms of reference for the Audit and Assurance Committee and therefore forms part of the Committee's annual self-evaluation of performance.

Objective 2: The process in place applies good practice in risk management (Continued)

Effectively communicated - The Risk Policy clearly signposts a role for all staff across the organisation in managing risk and this is enhanced by the availability of Risk Policy and the most up to date versions of the strategic risk register and directorate level risk registers. There is therefore limited opportunity, beyond SMT, to raise awareness about potential problems and share important information to ensure better problem solving, provide effective challenge and support and support effective escalation. This is therefore another area where further work is required to further develop existing arrangements. This is covered in more detail below.

Risk Management

Objective 2: The process in place applies good practice in risk management (Continued)				
Observation	**Risks**	**Recommendation**	**Management Response**	
Our review of individual directorate risk registers highlighted some variation in the way in which risks are being described and in the way that associated risk actions and controls are being documented, with some directorates adopting a succinct bullet point style and others adopting a more descriptive, narrative approach.	Without clarity on the way in which risks are presented, and the way in which mitigating actions and controls are described, there may be inconsistency in the way that risks are managed.	**R2** Consideration should be given to development of a procedure note which provides examples of the way in which risks should be articulated on the face of the relevant risk register (whether strategic, directorate or team) and demonstrates the way in which associated risk actions and controls should be documented in order to achieve further consistency in approach.	Agreed that there needs to be consistency and guidance will be produced. **To be actioned by:** Director of Strategy & Performance **No later than:** 31 October 2020	
			Grade	**3**

Objective 2: The process in place applies good practice in risk management (Continued)				
Observation	**Risks**	**Recommendation**	**Management Response**	
We noted that although progress in delivering mitigating actions - on both the strategic and directorate risk registers - is closely monitored, there are currently no individual responsibilities and target implementation dates set. In order to further develop the existing arrangements, we would suggest that once there is agreement on a uniform style of presentation for mitigating actions (see R2 above) then target completion dates should be set and overruns against these targets should be flagged in the monthly update report produced by each directorate – but only for those actions which do not appear in other plans and are therefore simply signposted from the risk register. By aligning mitigating actions created especially for the risk register with individual managers this will allow specific resource issues to be identified and discussed and should allow instances where there is a particularly heavy workload placed on specific individuals to be identified.	Without aligning specific responsibility and target completion dates for mitigating actions the pace of implementation may not be adequate to effectively manage the identified risk and resourcing issues may not be visible.	**R3** Consideration should be given to the alignment of individual mitigating actions to a named person (who may or may not be the overall risk owner) and target completion dates should be set for all mitigating actions associated with the risk register. However, this should only be the case for those actions created solely for the risk register, rather than a mitigating action which is simply signposted to an existing action on another plan and is therefore already subject to separate monitoring. Any variances against these target implementation dates should be highlighted and discussed to identify any barriers to successful implementation.	Agree that this can be implemented once agreed style of presentation i.e. bullet point actions are in place named individuals and timescales can be added where applicable**.** **To be actioned by:** All EMT members **No later than:** 31 October 2020	
			Grade	**3**

Risk Management

Objective 3: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and Council.

The ongoing alignment of current risks to strategic objectives will only be effectively maintained though effective scrutiny by the Audit and Assurance Committee and Council throughout the year. In addition, the annual development session provides protected time to consider the key risks facing the SSC and the way in which these are being managed in order to deliver strategic objectives.

The monthly update process is controlled centrally by the Strategy and Performance directorate under the executive oversight of the Director of Strategy and Improvement. The inclusion of risk management as a standing agenda item for EMT and OMT meetings demonstrates a clear commitment to the identification, assessment and management of risks.

From our attendance at the Audit and Assurance Committee meeting it was clear that there is a full discussion around risk management and a comprehensive presentation is provided with absolute transparency on key risks. It is also apparent that the is a great deal of experience in identifying and managing risks amongst the members of the Committee and this provides additional assurance that the risk management information presented will be subject to rigorous support and challenge.

The update report provided to the Audit and Assurance Committee signposts any movements in the risks so that there is full transparency and additional narrative is included to provide context. The updates also provide a stratified view of key risks across strategic risk categories.

It is clear form our discussions, and review of relevant documentation, that significant progress has been made in developing the process for identifying and managing risk since we delivered training to OMT managers in October 2019. The challenge now is to maintain the momentum created and to continue to develop the risk maturity of the risk management arrangements and to continue to embed this in the day to day work of managers and Council members.

Risk Management

Objective 3: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and Council. (Continued)				
Observation	**Risks**	**Recommendation**	**Management Response**	
Although the current configuration of the risk register includes a risk score (and an associated RAG status) for the residual risk level post-mitigation, the format does not currently identify instances where the residual risk level is above the risk appetite set by Council or the length of time which individual residual risk levels have been above the target risk level.	Without an indication of those risks where the residual risk level is above the agreed risk appetite, and the amount of time which these residual risks have been operating at above the agreed target risk level, the barriers to managing these risks down may not be challenged or rectified.	**R4** Consideration should be given to amending the format of the risk register to indicate the number of quarters where the residual risk has exceeded the agreed risk appetite level so that attention can be focused on these risks. We would suggest that this would also inform the discussion around risk at the annual development event mentioned above.	Agreed we can weight the appetite statements against the scoring matrix and add an additional column to the register that shows how many months residual score has remained the same or exceeded the appetite scoring. **To be actioned by:** Director of Strategy and Performance **No later than:** 31 October 2020	
			Grade	**3**

Aberdeen

45 Queen's Road
Aberdeen
AB15 4ZN

T: 01224 322100

Dundee

The Vision Building
20 Greenmarket
Dundee
DD1 4QB

T: 01382 200055

Edinburgh

Ground Floor
11-15 Thistle Street
Edinburgh
EH2 1DF

T: 0131 226 0200

Glasgow

100 West George Street
Glasgow
G2 1PP

T: 0141 471 9870

mha HENDERSON LOGGIE

hlca.co.uk | info@hlca.co.uk