AGENDA ITEM 9

CENTRAL SCOTLAND VALUATION JOINT BOARD

Subject: **2018/19 Internal Audit Review – Business Continuity Management Arrangements**
Meeting: **Central Scotland Valuation Joint Board**
Date: **01 February 2019**
Author: **Internal Audit Manager**

1. Introduction

1.1 This paper provides details of findings arising from the 2018/19 Internal Audit review of Business Continuity Management Arrangements.

2. Internal Audit Review of Business Continuity Management Arrangements

2.1 The Internal Audit Plan for 2018/19 was agreed by the Board on 29 June 2018. The Plan comprised reviews of:

- Business Continuity Management Arrangements;
- Arrangements for Recording, Monitoring, and Responding to Freedom of Information Requests; and
- Input to the Annual Governance Statement of Assurance Questionnaire process.

2.2 The report arising from work on the Business Continuity Management Arrangements is attached at **Appendix 1.**

2.3 We were able to provide Limited Assurance in relation to the adequacy of Business Continuity Management Arrangements, with six recommendations made to improve the framework of control.

2.4 All of the recommendations, including 'Responsible Owners' and 'Action Due' dates, were agreed with the Assessor and Electoral Registration Officer, and Internal Audit will follow up on the implementation of these recommendations during 2019/20.

3. RECOMMENDATIONS

3.1 The Board is asked to:

3.1.1 Note the findings arising from the 2018/19 Internal Audit review of Business Continuity Management Arrangements.

…….

Internal Audit Manager

Date: 24 January 2019

Author: Gordon O'Connor, Internal Audit Manager
Contact: tel 07872 048 030, email goconnor@clacks.gov.uk
Date: 24 January 2019

Appendices:

Appendix 1 – Internal Audit Report – Business Continuity Management Arrangements

List of Background Papers:

No papers were relied on in the preparation of this report in terms of the Local Government (Scotland) Act 1973.

Appendix 2

Business Continuity Management Arrangements

2018/19 Internal Audit Review

Limited Assurance

Report Recipients:
Assessor and Electoral Registration Officer

1. INTRODUCTION AND SCOPE

1.1 This review of Business Continuity Management (BCM) arrangements forms part of our 2018/19 coverage of Central Scotland Valuation Joint Board (CSVJB), agreed by the Valuation Joint Board in June 2018.

1.2 Internal Audit, in conjunction with the Assessor and Electoral Registration Officer, identified the key risks relating to BCM, and agreed a Terms of Reference for the review (**Annex 1**).

1.3 BCM is a 'holistic management process that identifies potential threats to an organisation and the impacts to operations those threats, if realised, might cause, and which provides a framework for building organisational resilience to safeguard the interests of its key stakeholders'[1].

2. AUDIT ASSURANCE AND EXECUTIVE SUMMARY

2.1 We can provide **LIMITED ASSURANCE** in relation to the adequacy of BCM arrangements (see **Annex 2** for assurance category definitions), and noted a number of areas where there was scope for improving the existing framework of control.

2.2 In particular, we found there to be a need to further embed risk management, through the performance of a Business Impact Analysis (BIA) at departmental level, and the development of a more robust corporate Business Continuity Plan (BCP).

2.3 A Business Continuity Team (BCT) has been established to develop, implement, and test BCM arrangements. We found, however, that no guidance and training has been provided to team members on the basic principles of BCM. In addition, there is no formal and comprehensive terms of reference to ensure transparency over the roles, accountabilities, and membership of the BCT.

2.4 A comprehensive and robust testing programme is not in place to ensure that BCM arrangements are operating efficiently, effectively, and to the required standard. At present, only the recovery of IT and email systems at premises out with the headquarters at Hillside House, Stirling, is subject to regular tests.

2.5 A summary of our recommendations is set out at **Section 4**, with more detail provided at **Section 3**.

3. AUDIT FINDINGS

Roles and Responsibilities

3.1 Responsibility for the strategic monitoring of BCM arrangements rests with the Operational Management Team (OMT). The OMT, which meets on a monthly basis, includes Senior Managers and representation from each business area (Electoral Registration and Property Valuation). Business continuity is a standing item on every OMT meeting agenda.

3.2 Responsibility for the day to day management of business continuity planning and recovery arrangements rests with the BCT. This includes the development of BCPs and establishment of a business continuity testing programme.

3.3 Discussions with staff highlighted that the BCT, which meets at least twice a year and more frequently if there are any emerging risks / issues, comprises of all OMT members, the Executive Assistant, and representation from the in-house IT Team.

3.4 We did note, however, that BCT roles and responsibilities are not formalised within a terms of reference[2]. In addition, membership of the BCT is not documented as attendees are not recorded on meeting minutes. To ensure transparency over the expectations, obligations, and membership of the BCT, we **recommend** that these issues are addressed.

[1] Source: International Standard for Business Continuity Management (ISO 22301)

[2] Note: We do acknowledge, however, that the roles of team members in the event of an emergency are documented within the corporate BCP.

Risk Management

3.5 Limited work has been undertaken to formally identify, prioritise, and risk assess all activities performed by each department, including resource requirements for each activity[3].

3.6 A periodic and comprehensive Business Impact Analysis (BIA) is an essential component of an effective BCM system as it identifies the impact a disruption to each activity will have on the organisation and the risks faced in relation to each activity. BIA findings guide decisions on the controls, continuity, and recovery plans required to minimise and prevent service disruption.

3.7 We **recommend** that a comprehensive BIA is undertaken by each department as a matter of priority and have summarised, at **Annex 3**, the process which should be followed. The findings stemming from these reviews should be used to inform the content of the corporate BCP. We have summarised, at **Annex 4**, our suggested format for the revised corporate BCP.

3.8 Although limited work has been undertaken at a departmental level in relation to risk management, consideration has been given by the corporate BCT to a variety of risks which may affect the organisation as a whole (eg, damage to CSVJB headquarters, cyber attacks, and loss of key operational staff through illness or leaving the organisation).

3.9 Various plans, policies, and controls have been developed to manage corporate risks. These include, for example: a corporate BCP; cybersecurity incident response plan; implementation of robust IT back-up and anti-virus protection regimes; and multiskilling of administration staff.

3.10 A high level review of a sample of the plans, policies, and controls in place did, however, highlight the following issues, which we **recommend** are addressed:

3.10.1 the corporate BCP has been designed primarily to account for the loss of headquarters at Hillside House, Stirling. Comprehensive guidance is not provided in relation to the actions which should be taken to manage and recover from other incidents which are equally as serious or probable (eg, power failure[4] or high staff absence due to a pandemic flu outbreak or sustained period of severe weather);

3.10.2 only one consolidated version of the corporate BCP exists, with this copy retained in a fire safe at Hillside House. To ensure that the plan is easily accessible in the event of a major incident at Hillside House, and to facilitate a timely and co-ordinated response which minimises service disruption, a second copy of the plan should be stored securely at an off-site location;

3.10.3 summarised versions of the corporate BCP are held at home by each member of the BCT, with the version held dependant on the role and seniority of that staff member. The following appendices are not, however, included in any of the summarised versions: Basic Equipment for Emergency Accommodation (Appendix E); Incident Logging Form (Appendix F); Health and Safety Guidelines (Appendix G); and IT and Furniture Inventories (Appendices H and I). These appendices do not contain sensitive information, and are a useful reference point in the event of an incident, especially in cases where the consolidated BCP can not be obtained from the fire safe at Hillside House. Consideration should, therefore, be given by Management to the inclusion of this information in all summarised versions of the BCP; and

3.10.4 the cybersecurity incident response plan remains in draft. This plan should be reviewed and finalised by the OMT to ensure the consistent application of robust controls when managing, investigating, and remediating IT security incidents.

[3] Note: We do acknowledge, however, that the Electoral and Administration Team develop a Contingency Planner and Risk Register prior to each electoral event, with a priority list also in place for the recovery of CSVJB's IT systems.

[4] Note: The IT Systems Administrator advised that the IT Working Group have considered the steps required to ensure that a basic level of service is provided during electoral periods in the event of a power failure / outage. It was acknowledged, however, that these steps have not been formally documented.

Training

3.11 BCT members have been the main recipients of training on BCM, with two disaster recovery rehearsal exercises undertaken since December 2017 to clarify the team's roles and responsibilities in relation to, and the workability of, the corporate BCP (as per paragraph 3.14).

3.12 We did, however, note that BCT members have not been provided with any training or information on the basic principles of BCM (eg, how to undertake a BIA or develop a BCP). To ensure that staff are suitably equipped to identify and assess critical business functions, and to subsequently develop appropriate plans to minimise the risk of service disruption, we **recommend** that this issue is addressed.

Testing of Business Continuity Plans

3.13 Robust testing programmes should ensure that business continuity arrangements are operating efficiently, effectively, and to the required standard. They should also provide a formal structure against which to identify training requirements and lessons learned (for inclusion within the amended corporate BCP).

3.14 Our review of testing arrangements to date highlighted that disaster recovery rehearsal exercises were undertaken on 14 December 2017 and 25 July 2018. These exercises focussed solely on the recovery, rather than the operation, of IT and email systems should staff have to relocate to alternative premises[5].

3.15 As per paragraphs 3.10.1 and 3.10.4 above, no guidance is in place setting out the actions which should be taken to manage and recover from incidents other than the loss of CSVJB headquarters or a cyber security attack. Consequently, no tests have been undertaken on arrangements for dealing with incidents such as power failure or high staff absence due to severe weather.

3.16 We therefore re-iterate our **recommendation** that the corporate BCP is amended to include all serious and probable incidents. Once finalised, a formal, comprehensive, risk based, testing programme should be prepared and implemented, setting out the plans which are to be tested and the nature and frequency of these tests. Consideration should be given to the importance of the area under review when determining the priority, nature and frequency of tests.

[5] Note: We do acknowledge, however, that a test day to consider cyber attacks is scheduled for 12 December 2018, with a further test day scheduled for February 2019 to assess plans for the live operation of the Electoral Registration and Electoral Management (EROS) IT system at alternative premises.

4. RECOMMENDATIONS AND ACTION PLAN

Rec. No.	Recommendation	Reason for Recommendation	Agreed Management Action	Responsible Owner	Action Due
1.	A terms of reference should be established for the Business Continuity Team, and the format of meeting minutes amended to include the names of all attendees. **Report Paragraph: 3.4**	To ensure transparency over the expectations, obligations, and membership of the BCT.	**Recommendation Accepted** The plan itself sets out the remit of the Business Continuity Team in the event of the plan being invoked, and their roles and responsibilities. We will establish a terms of reference for the team that reviews the plan on a regular basis, as well as formally noting the membership of the review team.	Assessor	February 2019
2.	A formal and comprehensive Business Impact Analysis should be completed by all departments. The findings stemming from these reviews should be used thereafter to inform the content of the corporate BCP. **Report Paragraph: 3.7**	To identify and prioritise activities critical to service delivery; raise awareness of the areas for which robust controls, continuity, and recovery plans are required; and to minimise the risk of service disruption.	**Recommendation Accepted** Agreed that this needs to be formally documented.	Operational Management Team	June 2019
3.	The issues relating to the corporate Business Continuity Plan should be addressed. **Report Paragraphs: 3.7 and 3.10.1 to 3.10.3**	To ensure the consistent, timely, and transparent application of robust controls, and to minimise the risk of service disruption.	**Recommendation Accepted** Business Continuity Plan to be updated once Business Impact Assessments have been completed.	Operational Management Team	July 2019
4.	The Cybersecurity Incident Response Plan should be reviewed and finalised by the Operational Management Team. Once finalised, the Plan should be disseminated to relevant staff, with training provided if required. **Report Paragraph: 3.10.4**	To ensure the consistent application of robust controls when managing, investigating, and remediating IT security incidents.	**Recommendation Accepted** The Cybersecurity Incident Response Plan is to be finalised at the Operational Management Team meeting in February.	Operational Management Team	February 2019
5.	Training on the principles of Business Continuity Management should be provided to all members of the Business Continuity Team. **Report Paragraph: 3.12**	To ensure that staff are suitably equipped to identify and assess critical business functions, and to subsequently develop appropriate plans to minimise the risk of service disruption.	**Recommendation Accepted** Suitable training to be identified.	Assistant Assessor	April 2019
6.	A formal, comprehensive, risk based testing programme should be prepared and implemented for business continuity arrangements. **Report Paragraph: 3.16**	To ensure that comprehensive contingency plans are in place, and that they remain workable, proportionate, and effective in minimising service disruption.	**Recommendation Accepted** A working test of the Electoral Software is scheduled for February 2019. Valuation test to be scheduled in due course.	Executive Assistant	August 2019

ANNEX 1

Terms of Reference

Service:	Central Scotland Valuation Joint Board	**Audit Year:**	2018/19
Assessor and Electoral Registration Officer:	Pete Wildman	**Audit Manager:**	Gordon O'Connor
Audit Area:	Business Continuity Management Arrangements	**Lead Auditor:**	Sandy Carmichael

SCOPE

The scope of this review was to evaluate and report on the robustness and completeness of Central Scotland Valuation Joint Board's Business Continuity Management arrangements. This review formed part of our 2018/19 Internal Audit Plan agreed by the Valuation Joint Board on 29 June 2018.

KEY RISKS

The following were identified as key risks:

- gaps in the business continuity planning and recovery framework, resulting in unacceptable service disruption;
- lack of clarity in roles, responsibilities, and documented plans, leading to a fragmented and / or ineffective recovery response; and
- inadequate arrangements for testing business continuity plans, resulting in a failure to identify and address plans that are neither practical nor actionable.

REMIT ITEMS

We developed our work-plan to obtain the necessary evidence to provide assurance that appropriate systems were in place to mitigate the above risks. This was achieved by reviewing:

1. overarching arrangements for establishing business continuity and recovery plans. In particular:
    - roles and responsibilities;
    - arrangements for identifying and risk assessing critical systems and activities; and
    - ownership of, and accountability for, the completeness, proportionality, and effectiveness of the framework of Business Continuity Plans.
2. the availability of guidance, training, and support to staff responsible for implementing business continuity plans; and
3. arrangements for testing the adequacy and robustness of business continuity plans.

ANNEX 2

DEFINITION OF ASSURANCE CATEGORIES

Level of Assurance	Definition
Substantial assurance	Largely satisfactory risk, control, and governance systems are in place. There may be some scope for improvement as current arrangements may undermine the achievement of objectives or leave them vulnerable to error or abuse.
Limited assurance	Risk, control, and governance systems have some satisfactory aspects. There are, however, some significant weaknesses likely to undermine the achievement of objectives and leave them vulnerable to an unacceptable risk of error or abuse.
No assurance	The systems for risk, control, and governance are ineffectively designed and operated. Objectives are not being achieved and the risk of serious error or abuse is unacceptable. Significant improvements are required.

ANNEX 3

SUGGESTED BUSINESS IMPACT ANALYSIS PROCEDURE

The following is a list of suggested actions that each department should undertake to facilitate identification of critical activities and the threats posed to the successful operation of these activities:

1. Clearly define all responsibilities for the department. For example, the Electoral Registration and Administration Team are responsible for: preparing and publishing the annual Register of Electors; maintaining a list of absent voters; assisting Returning Officers with the preparation of poll cards, proxy poll cards, and addressing for postal votes; etc.

2. Document the key processes required to satisfy each of the departmental responsibilities.

3. Detail the resources required to perform each activity. For example:

   - People: who undertakes the activity; what skills / level of expertise is required by these members of staff; and what is the minimum staffing levels with which the activity could be undertaken;

   - Premises: from where is the activity undertaken, and what facilities are required to carry out the activity;

   - Equipment / Documentation: what IT systems / applications, records, and communication systems are essential to carry out the activity; and

   - Providers: who are the key suppliers / contractors for the equipment / IT systems etc required to undertake the activity.

4. Identify the potential consequences of disruption to each activity. The consequences can be categorised according to impact on Service User, Breach of Statutory Duty, Impact on Staff, and Financial Impact. The consequences should be given a High, Medium or Low impact rating.

5. Identify the criticality of the activity based on consideration of the consequences of disruption to the activity. An overall criticality rating should be allocated based on consideration of the category impact ratings identified at step 4. For example: 1 – Not Critical; 2 - Moderately Critical; and 3 – Critical / Vital.

6. Identify the maximum permissible time the activity can be suspended before consequences become high and allocate a rating. For example, 4 if activity can only be suspended for less than 24 hours and 1 if activity can be suspended for in excess of 5 working days.

7. Identify the priority of the activity compared to other activities within the department. The 2 risk ratings noted at steps 5 and 6 could be multiplied to identify an overall score.

8. Identify any dependencies with other activities.

9. Identify potential failure points for each critical activity.

10. Identify controls to limit the potential for failure and to ensure minimal service disruption. This should include the development of business continuity plans.

ANNEX 4

SUGGESTED FORMAT FOR A BUSINESS CONTINUITY PLAN

Section	Comments
Title Page	• Date Plan prepared and next review date; • Name of Officer(s) responsible for preparing and reviewing Plan; and • Distribution list.
Contents Page	• List of sections and where information can be found.
Purpose / Objectives of Plan	• Description of what the plan aims to achieve. For example: respond to a disruptive incident; maintain delivery of critical activities / services during an incident; and return to business as usual.
Activation of the Plan	• Details of the person(s) that will take the decision to activate the plan and the circumstances in which the plan will be invoked. For example: denial of access, or damage to, premises; ICT failure or cyber attack; loss of key staff or skills due to severe weather or high absenteeism due to illness; loss of power; etc.
Critical Activities Checklist	• List of the critical activities in order of importance and the recovery timeframe for each activity.
Critical Activity Analysis and Restoration Procedures	• Each critical activity should have a separate sheet setting out the following information: ➢ A brief description of the activity; ➢ Officer responsible for leading on the activity; ➢ The potential impact on the organisation if this activity is interrupted; ➢ The likelihood of interruption to the activity; ➢ Recovery timeframe for the activity; ➢ Minimum number of staff required to recover the function, including required skills and knowledge and alternative sources to replace the usual staff; ➢ Details of data and IT requirements, back up, and recovery processes (including where back ups are located and how they will be restored); ➢ Premises to which staff can relocate; ➢ Equipment required to undertake the activity and location of suitable replacements; and ➢ Key stock and supplies requirements, including processes for replenishing these items.
Response Actions	• The sequence of actions required to maintain minimum standards of service when significant risks are realised and to restore the function to full capacity. A separate sheet should be developed setting out the action to take for each type of event (eg, denial of access, or damage to, premises; ICT failure; loss of key staff; loss of power, etc).
Contacts List	• List of contact details for all staff with responsibility for implementing / using the plan and relevant outside agencies (eg key suppliers and contractors).

Source: Adapted from Camden - Basic Business Continuity Management Plan Template.