Business Assurance and Risk Management

Risk Management and Business Continuity Planning - FINAL

Auditors

Maggie Gibb, Head of Business Assurance (and Chief Internal Auditor)

Selina Harlock, Audit Manager

Juan Fosco, Audit Manager

Axolile Kopman, Assistant Manager

Management Summary

Introduction

The Business Continuity and Risk Management audit was undertaken as part of the 2022/23 Internal Audit plan. This area was included in the plan at the Audit Committee's request and due to the significance of risks related to the area in Buckinghamshire & Milton Keynes Fire Authority (BMKFA) Risk Register. Under the Civil Contingencies Act 2004, the Authority has a statutory duty to maintain business continuity plans to ensure they can maintain services in the event of an emergency.

Due to the reliance placed on ICT for the operation of services within the Authority, ICT service resilience and disaster recovery provisions are critical components of business continuity. Disaster Recovery (DR) planning enables the recovery of ICT systems in the event of disruption impacting the data centre or server room hosting the Authority's IT systems. Given that information and communication technology plays an increasingly important role in delivering Authority services, the ability to recover these systems promptly is essential.

Audit Objective

Internal Audit's objectives for this audit were to provide an evaluation of, and an opinion on, the adequacy and effectiveness of current controls over Risk Management and Business Continuity Planning and guide how to improve the current controls going forward.

This will serve as a contribution toward the overall opinion on the system of internal control that the Chief Internal Auditor is required to provide annually. It also provides assurance to the Section 112 officer that financial affairs are being properly administered.

Scope of work

The agreed scope of this audit was:

- Risk Management Framework;
- Risk Identification and Evaluation;
- Risk Record and Management;
- Risk Monitoring;
- Policies, Procedures & Business Continuity Plans;
- Roles & Responsibilities;
- Business Continuity Testing;
- Lessons Learned;
- Monitoring & Reporting;
- Anticipated Industrial Action Plans, and
- ICT Disaster Recovery.

This audit only considered the controls in place at the time of the audit.

Table 1: Overall Conclusion

Overall conclusion on the system of internal control being maintained	**Reasonable**

RISK AREAS	AREA CONCLUSION	No. of High Priority Management Actions	No. of Medium Priority Management Actions	No. of Low Priority Management Actions
Risk Management				
Risk Management Framework	**Substantial**	**0**	**0**	**0**
Risk Identification and Evaluation	**Substantial**	**0**	**0**	**0**
Risk Record and Management	**Substantial**	**0**	**0**	**0**
Risk Monitoring	**Substantial**	**0**	**0**	**0**
Business Continuity Planning				
Policies, Procedures & Business Continuity Plans	**Reasonable**	**0**	**1**	**0**
Roles & Responsibilities	**Reasonable**	**0**	**1**	**0**
Business Continuity Testing	**Limited**	**1**	**0**	**0**
Lessons Learned	**Reasonable**	**0**	**1**	**0**
Monitoring & Reporting	**Reasonable**	**0**	**1**	**0**
Anticipated Industrial Action Plans	**Substantial**	**0**	**0**	**0**
ICT Disaster Recovery	**Limited**	**1**	**0**	**1**
Total		**2**	**4**	**1**

Appendix 1 defines the grading for each of the conclusions given.

Risk Management

Risk Management Framework

The Authority has a Corporate Risk Management Policy approved by the Fire Authority Executive Committee on 24 March 2021. Among others, the Policy sets out the following:

- Risk Management Definitions;
- Risk Appetite;
- Governance Structures;
- Roles and Responsibilities;
- Risk Management Processes and Methods;
- Consultation /Publication / Communication, and
- Impact Assessments.

The overall responsibility for risk management sits with the Authority's Strategic Management Board (SMB), which is responsible for reviewing, moderating and owning the risks designated as 'corporate'. The Chief Executive/Chief Fire Officer is responsible for day-to-day risk management.

The SMB has delegated responsibility to the Performance Monitoring Board (PMB) for reviewing and evaluating risks and acts as the escalation point for Directorate-level risks.

The Business Transformation Board (BTB) is also responsible for reviewing and evaluating risks and acts as the escalating point for project-related risks. Reviewing the Corporate Risk Management Policy and the Authority's Risk Registers, we confirmed that there is an appropriate delegation of risk management.

We confirmed that risk management is a regular agenda item at the relevant governance structures, such as the Strategic Management Board (SMB) and the Overview and Audit Committee (OAC). Reviewing the corporate risk management report prepared by the Corporate Planning Manager for the OAC meeting held in November 2022, we confirmed that risk management is covered and deliberated at the Authority's appropriate governance structures.

The Authority has a Public Safety Plan and the Corporate Plan for 2020-2025 that also informs the Authority's risk framework. For example, the Corporate Plan sets out strategic objective number four: *"To offer best value for money to our residents and businesses & ensure that the Service is compliant with regulatory requirements and recognised 'good practice' standards and can readily evidence this at all times"*. We confirmed that a risk was identified in the Corporate Risk Register concerning this strategic objective under Information Management/Security failure - to comply with statutory or regulatory requirements.

Risk Identification and Evaluation

The Corporate Risk Management Policy defines the risk appetite as the amount of risk the Authority is willing to tolerate relative to the size, nature, and degree of uncertainty associated with identified threats and opportunities. The Policy states that risks attracting a combined score of 20 or more on the Risk Scoring Matrix will be considered intolerable by the Authority and prioritised for treatment to eliminate or reduce the risk to acceptable levels. The Policy also indicates

that the ownership of the Risk Appetite at the Authority sits with the Fire Authority Executive Committee, and the risk appetite statement applies to the Authority at large. Reviewing the risk registers in place, we confirmed that for those risks that remained high after mitigating controls were suggested, further action plans were also suggested, and the actions are tracked as 'ongoing'.

Regarding training, we obtained a PowerPoint presentation on Corporate Risk Management utilised to provide training. The Corporate Planning Manager and the ICT Service Desk Manager conducted a specific training session in July 2021 for the new Members of the Fire Authority. Management confirmed that training is provided as and when there is a new starter joining the Authority. The training covers, amongst others:

- Risk management process;
- Risk scoring matrix, and
- Risk governance.

Upon our review of the Corporate Management Risk policy and risk registers, we noted that all grades of staff could identify risks. We also noted that the risks were escalated to the PMB should they require further action, and a responsible individual for managing the identified risk is assigned to the risk register.

Operational risk management is defined and coordinated. We reviewed the Directorate/corporate risk registers and confirmed that operational managers are responsible for managing operational risks by being assigned as risk owners.

Risk Recording and Management

Reviewing the Authority's risk registers, we confirmed that the risks were consistently scored using the quantitative approach method. The risks identified were assessed in terms of likelihood and severity (impact) for both inherent risk (gross risk) and residual risk (net risk). These were converted into numerical terms.

We reviewed the OAC reports and agendas for the 16 March, 20 July, and 09 November 2022 meetings. Upon review of the corporate risk register presented, we confirmed that action plans were suggested for the risks identified that required further action and were tracked on an ongoing basis. We confirmed this in the corporate risk management report the Corporate Planning Manager presented.

We reviewed the minutes of the Performance Monitoring Board (PMB) meeting held on 03 February, 09 June, and 29 September 2022. We noted that the risks escalated from the directorate management meetings were discussed. For example, on the 03 February 2022 meeting, a risk was escalated around information on Site Specific Risk Information (SSRI) and a further delay to the delivery of the related project.

We reviewed the extract of the meeting minutes of the Business Transformation Board (BTB) meeting held on 11 August, 08 September, and 06 October 2022. Upon review, we noted that the project risks escalated from the portfolio management office were discussed.

Reviewing the risk registers, we noted a clear distinction between types of risks. The risk registers were divided into prevention, response & resilience risk register, corporate risk register and directorate or departmental risk registers. We noted that the efforts SMB are focused on the Strategic risks, demonstrating appropriate prioritisation of senior management's time.

Corporate Planning provides appropriate templates and systems for analysing, evaluating, recording, and reporting risks identified at directorate and corporate levels. The Project Management Office (PMO) will do the same for project risks. We reviewed the directorate/departmental risk register, corporate risk register, and technology, transformation and PMO risk register, which highlighted that a systematic approach to risk management was continuously applied concerning risk identification, recording, assessment and analysis.

Risk Monitoring

Formal review and reporting of corporate risks are undertaken at every PMB and SMB meeting and the Authority's OAC. We reviewed the minutes of the PMB meetings held on 03 February, 09 June, and 29 September 2022. We confirmed that risk registers are reviewed and deliberated on this platform. We also reviewed the Board papers presented to the PMB corresponding to these meetings. The Board papers provided an update on the current status of identified corporate risks.

We also reviewed the extract of the meeting minutes for the Strategic Management Board (SMB) held on 23 August, 20 September, and 18 October 2022. The meeting minutes for 15 November 2022 were not yet available at the time of the audit; however, we reviewed the Board paper presented to the SMB, and we noted that risk registers are reviewed and deliberated in this platform. We also reviewed the Board papers presented to the SMB corresponding to these meetings and confirmed they provided an update on the current status of identified corporate risks.

Furthermore, we reviewed the minutes of the OAC meetings held on 16 March and 20 July 2022. Upon review, we noted that risk registers are reviewed and deliberated in this platform. We also reviewed the Board papers presented to the OAC corresponding to these meetings and confirmed they provided an update on the current status of identified corporate risks.

Business Continuity

Policies, Procedures & Business Continuity Plans

We reviewed the Business Continuity Policy and guidance (August 2022 version), which includes areas relevant to business continuity, including components such as the following:

- Production of the business continuity plans;
- Testing of the plans;
- Business continuity events, and
- Impact assessments.

As of December 2022, the Authority has 16 departments and 19 fire stations, each with a business continuity plan. We obtained copies of the plans for each department and fire station. We confirmed the existence, although we observed plans not being reviewed recently (more details are included in Table 2 below). Through the review of the business continuity policy, we also noted that the Authority pursues to align with the standards of Business Continuity Management as defined by ISO 22301 and the Business Continuity Institute Good Practice Guidelines.

Roles & Responsibilities

The Chief Fire Officer has ultimate responsibility for Business Continuity. This includes developing and implementing plans to anticipate, address and mitigate the effects of various business interruptions. The Resilience and Business Continuity Manager is tasked with the day-to-day roles and responsibilities regarding business continuity across the Authority. The job description for this role clearly states what is expected of the individual who occupies the role.

We obtained a copy of the Certificate of the Business Continuity Institute (CBCI) for the Resilience & Business Continuity Manager issued on 21/02/2020. The certification is valid for three years from the test's date and is subject to an annual maintenance fee.

Anticipated Industrial Action at the Authority

We obtained the industrial action plan (documented procedure), dated August 2022, and noted that it includes an appendix for 'industrial action planning'. This outlines what the Authority would do should the industrial action materialise. Also, industrial action planning is broken into a number of days as to what should happen on a particular day of a strike.

ICT Disaster Recovery

The Authority has an Information Communications (ICT) departmental business continuity plan issued in August 2022. The next review date is July 2023.

The Head of Technology, Transformation & PMO, the ICT Manager, and the ICT Service Desk Manager are responsible for ICT business continuity at the Authority. The Chief Fire Officer has ultimate responsibility for all aspects of Business Continuity.

The ICT Service Desk Manager is a nominated officer responsible for activating the ICT BCP during working hours. Out of hours or if none of the nominated persons is available, then the Duty Group Commander, in conjunction with the on-call ICT, will be contacted to decide if activation of the plan is appropriate.

We noted that as part of the ICT Disaster Recovery plan testing (last performed in 2019), lessons learned were identified due to the testing.

We were provided with the server screenshots and confirmed that ongoing backups are performed daily on data held within.

Table 2: Detailed Audit Findings and Management Action Plan

Finding 1: Business Continuity Plans - Testing	**Risk Rating**	**Agreed Management Actions**
We could not obtain evidence to support that the BCPs were tested annually as the business continuity guidance requires. Management indicated that this was not done due to capacity constraints in the business continuity section. Without developing and implementing a formal testing program, there is the risk that appropriate levels of testing are not undertaken to establish the ability of the BCP to support an effective and efficient response to business disruption. The lack of business continuity tests increases the risk that existing plans are not fit for purpose. The Authority would fail in its statutory duty to maintain services in an emergency or major incident. We recommend that, once all BCPs have been developed and approved, management introduce a risk-based testing program for BCPs. This should include a range of tests, including live testing and simulations of different scenarios. Testing must be targeted at areas most susceptible to an incident and/or would suffer the most adverse consequences. Plans should be confirmed as appropriate following the completion of tests.	**H**	**Action:** An exploratory testing programme, targeting those functions considered most at risk, will be developed and piloted during 23/24. Also, the options and associated costs and resources required to develop, implement, and sustain a fully recordable business continuity testing and exercising programme will be investigated during 23/24. **Officer responsible:** Station Commander Resilience & Business Continuity **Date to be implemented by:** 31 March 2024 for completion of pilot and review of future development options.
Finding 2: ICT Disaster Recovery Plan - Testing	**Risk Rating**	**Agreed Management Actions**
We confirmed that the ICT disaster recovery (DR) Plan was last tested in 2019. BMKFA should consider testing the ICT DR Plan annually to help the Authority identify and fix inconsistencies and flaws before they become full-blown problems. The authority should consider filling vacancies in the ICT in a timely manner to ensure that the unit is at full establishment to deliver on its tasks including Disaster Recovery Testing. BMKFA is faced with the risk of not being certain if the DR Plan is still functional, and also, there is a risk of missed opportunities.	**H**	**Action:** Vacant posts to be filled and ensure that ICT is at establishment. **Officer responsible:** ICT Manager **Date to be implemented by:** 31st March 2023 Latest Update: Two apprentices have been employed to assist with first line support, but it could take them up to 2 years to gain the correct skills and level of knowledge. **Action:** Test the ICT disaster recovery plan **Officer responsible:** ICT Manager **Date to be implemented by:** 31 March 2024

<table>
<tr><th>Finding 3: Business Continuity - Employee Awareness and Training</th><th>Risk Rating</th><th>Agreed Management Actions</th></tr>
<tr><td>We confirmed that the business continuity manager holds a Certificate of the Business Continuity Institute (CBCI). However, there has been limited awareness training provided for relevant staff (typically responsible managers) in relation to Business Continuity.

Formal business continuity training is not developed and rolled out to responsible managers. This could be in the form of an e-Learning module. There is no active promotion by senior management to emphasise the importance of business continuity. This could be in the form of email campaigns or staff newsletters.

If a positive business continuity culture is not embedded within the Authority, there is the risk that staff members will not have the required level of knowledge and will not fully understand their responsibilities effectively should BCPs be invoked.</td><td>M</td><td>Action: An e-Learning package will be developed in the short term. However, a full restructure of Business Continuity Management processes is required to fully meet the recommendations which will include the development and implementation of a business continuity awareness & training programme.

Officer responsible: Station Commander Resilience & Business Continuity

Date to be implemented by:

31 October 2023 (for the e-learning package)

31 March 2024 (for future development options / proposals).</td></tr>
<tr><th>Finding 4: Business Continuity Plans Review</th><th>Risk Rating</th><th>Agreed Management Actions</th></tr>
<tr><td>As of December 2022, the Authority had a total of sixteen directorates and nineteen fire stations; each had a BCP. Whilst the existence was confirmed, no evidence could be obtained that the BCPs were reviewed by the planned date. Management indicated an issue with the capacity of the business continuity section.

Out of nineteen fire station BCPs, we noted that sixteen were not reviewed as planned:

<table>
<tr><th>#</th><th>Fire Station</th><th>Issue Date</th><th>Planned Review Date</th></tr>
<tr><td>1</td><td>Amersham</td><td>14-Apr-21</td><td>12-Apr-22</td></tr>
<tr><td>2</td><td>Aylesbury</td><td>27-Jan-17</td><td>12-Mar-20</td></tr>
<tr><td>3</td><td>Brill</td><td>Sep-19</td><td>Sep-20</td></tr>
<tr><td>6</td><td>Haddenham</td><td>Sep-19</td><td>Sep-20</td></tr>
<tr><td>7</td><td>Marlow</td><td>04-Jan-16</td><td>Nov-18</td></tr>
<tr><td>8</td><td>Olney</td><td>Jul-19</td><td>Jul-20</td></tr>
<tr><td>9</td><td>Stokenchurch</td><td>04-Jan-16</td><td>Nov-18</td></tr>
<tr><td>11</td><td>Beaconsfield</td><td>14-Apr-21</td><td>12-Apr-22</td></tr>
</table></td><td>M</td><td>Action: A full restructure of Business Continuity Management structures and processes is required to fully meet the recommendations which will include the development and implementation of fully auditable Business Continuity Plans that align to current standards and good practice. In the meantime, Business Continuity Plan review completions will be monitored on an ongoing basis and added to the suite of performance measures reported to the Authority's Executive Committee.

Officer responsible: Station Commander Resilience & Business Continuity

Date to be implemented by: Inclusion of BCP review completions in performance measures by 30 April 2023.</td></tr>
</table>

12	Broughton	26-Mar-20	Mar-20
13	Chesham	07-Aug-17	Nov-18
14	Great Missenden	04-Jan-16	Nov-18
15	High Wycombe	04-Jan-16	Nov-18
16	Newport Pagnell	20-May-15	Apr-17
17	Princes Risborough	04-Jan-16	Nov-18
18	Waddesdon	Jul-19	Jul-20
19	Winslow	Jul-19	Jul-20

Out of sixteen directorates BCPs, we noted that eleven were not reviewed as planned:

#	Directorates	Issue Date	Planned Review Date
1	Finance & Assets (includes Finance, Property, Payroll, Fleet, Procurement)	01-Apr-18	Apr-19
2	Organisational Development	06-Mar-18	05-Jan-22
3	Operational Assurance	04-Jan-16	Nov-18
4	Operational Training	30-Jan-18	Dec-20
5	Buckinghamshire Protection	09-Aug-16	Nov-18
6	Milton Keynes Protection	13-Mar-20	May-21
7	Resource Management Team	27-Jul-16	Jul-20
8	Policy & Resilience	04-Feb-20	Feb-21
9	Technical	28-Jul-20	Jul-21
10	Health & Safety	09-Aug-16	Mar-21
11	Data Intelligence Team	04-Jan-16	Nov-18

There is a risk that critical changes might be missed due to failure to update the BCPs and result in an ultimate failure to recover should an event.

BMKFA should update the BCPs annually for all critical functions or as and when there is a critical change in the process.

Full restructure of business continuity processes – date to be confirmed following investigation of potential options and associated costs and resource requirements (delivery of these by 31 March 2024).

Finding 5: BCP Lessons Learned	Risk Rating	Agreed Management Actions
We noted that the lessons learned were not identified since the BCPs were not tested since 2019. The Authority cannot, therefore, identify the BCP's positive or negative experiences due to failure to perform the BCP testing. The Authority should ensure that lessons learnt are identified once the BCPs are tested to ensure that the organisation doesn't repeat the same mistakes. The outcomes of these tests should be formally documented and identified 'as lessons learnt.	**M**	**Action:** A full restructure of the Business Continuity Management structures and processes is required to fully meet the recommendations, which would include the development and implementation of a business continuity system that formally records learning and any required actions from learning following exercises and business continuity events. In the meantime, the capture of learning opportunities will be included in the pilot testing programme specified under Finding 3 above. **Officer responsible:** Station Commander Resilience & Business Continuity **Date to be implemented by:** Piloting - 31 March 2024. Full restructure of BCM to be confirmed following investigation of potential options and associated costs and resource requirements (delivery of these by 31 March 2024).
Finding 6: BCP Monitoring and Reporting	**Risk Rating**	**Agreed Management Actions**
While we noted that BCP is discussed at a PMB forum as an overlap as part of risk management reporting, we confirmed that no regular reports regarding business continuity are produced. The Authority should ensure that it is effectively monitoring the business continuity management system and seek assurance that it remains effective and fit for purpose. Consideration should be given to regularly updating various governance forums available at the Authority on current business continuity activities. This could include but not be limited to: • An annual report on the business continuity management system; • Any activation of business continuity plans and the lessons learned; • Outcomes from business continuity tests; and	**M**	**Action:** A full restructure of Business Continuity Management structures and processes is required to fully meet the recommendations which would include the development and implementation of a reporting system to provide business continuity performance information e.g. number of plans out of review date, number of plans exercised. **Officer responsible:** Station Commander Resilience & Business Continuity

• Outcomes from any dip sampling of business continuity plans. There is an increased risk that an ineffective or inappropriate business continuity system is not identified through regular monitoring and reporting, placing the Authority at risk of being unable to carry out its statutory duties effectively in the event of an incident or emergency.		**Date to be implemented by:** The outcomes of ongoing monitoring of business continuity plan reviews and testing will be reported to PMB on an annual basis (April 24 for first report). Future reporting system development options / proposals 31 March 2024)
Finding 7: ICT Disaster Recovery Plan - Roles and Responsibilities	**Risk Rating**	**Agreed Management Actions**
Upon review of the BMKFA ICT disaster recovery plan, we noted that although there are names and job titles of the individuals with the responsibilities of activating the plan mentioned within the ICT disaster recovery plan, there are no further contact details. Those individuals are the Head of Technology Transformation & PMO, ICT (ICT Manager), and ICT (Service Desk Manager). BMKFA should include the contact numbers of the individuals with the responsibilities of activating the ICT DR Plan within the plan enabling ease of getting contact details in case of a disaster. There is a risk that staff would not know how to contact key staff members in the event of a disaster.	**L**	**Action:** Information to be added to the document on resilience direct. **Officer responsible:** ICT Manager **Date to be implemented by:** 1 March 2023

Appendix 1: Definition of Conclusions

Key for the Overall Conclusion:

Below are the definitions for the overall conclusion on the system of internal control being maintained.

	Definition	Rating Reason
Substantial	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	The controls tested are being consistently applied and risks are being effectively managed. Actions are of an advisory nature in context of the systems, operating controls and management of risks. Some medium priority matters may also be present.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Majority of actions are of medium priority but some high priority actions may be present.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	There is an inadequate level of internal control in place and/or controls are not being operated effectively and consistently. Actions may include high and medium priority matters to be addressed.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	The internal control is generally weak/does not exist. Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Actions will include high priority matters to be actioned. Some medium priority matters may also be present.

Management actions have been agreed to address control weakness identified during the exit meeting and agreement of the Internal Audit report. All management actions will be entered onto the Pentana Performance Management System and progress in implementing these actions will be tracked and reported to the Strategic Management Board and the Overview & Audit Committee.

We categorise our management actions according to their level of priority:

Action Priority	Definition
High (H)	Action is considered essential to ensure that the organisation is not exposed to an unacceptable level of risk.
Medium (M)	Action is considered necessary to avoid exposing the organisation to significant risk.
Low (L)	Action is advised to enhance the system of control and avoid any minor risk exposure to the organisation.

Appendix 2: Officers Interviewed

The following staff contributed to the outcome of the audit:

Name:	Title:
Stuart Gowanlock	Corporate Planning Manager
Suzanne Connolly	Resilience & Business Continuity Manager
Lewis Higgins	ICT Service Desk Manager

The Exit Meeting was attended by:

Name:	Title:
Stuart Gowanlock	Corporate Planning Manager
Lewis Higgins	ICT Service Desk Manager

The auditors are grateful for the cooperation and assistance provided from all the management and staff who were involved in the audit. We would like to take this opportunity to thank them for their participation.

Appendix 3: Distribution List

Draft Report

Name:	Title:
Stuart Gowanlock	Corporate Planning Manager
Suzanne Connolly	Resilience & Business Continuity Manager
Lewis Higgins	ICT Service Desk Manager
Mark Hemming	Director of Finance and Assets

Final Report as above plus:

Jason Thelwell	Chief Finance Officer
Ernst and Young	External Audit

Audit Control:

Closing Meeting	12 December 2022
Draft Report	31 January 2023
Management Responses	10 February 2023
Final Report	22 February 2023

Disclaimer

Any matters arising as a result of the audit are only those, which have been identified during the course of the work undertaken and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that could be made.

It is emphasised that the responsibility for the maintenance of a sound system of management control rests with management and that the work performed by Internal Audit Services on the internal control system should not be relied upon to identify all system weaknesses that may exist. However, audit procedures are designed so that any material weaknesses in management control have a reasonable chance of discovery. Effective implementation of management actions is important for the maintenance of a reliable management control system.

Contact Persons

Maggie Gibb, Head of Business Assurance

Phone: 01296 387327

Email: maggie.gibb@buckinghamshire.gov.uk

Selina Harlock, Audit Manager

Phone: 01296 383717

Email: selina.harlock@buckinghamshire.gov.uk