Internal Audit

FINAL

Dacorum Borough Council

Assurance Review of Business Continuity

2021/22

May 2022

Executive Summary

OVERALL ASSESSMENT

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

Loss of major hardware/data centre (failure / theft / flood)

KEY STRATEGIC FINDINGS

An exercise to review and update the Council's Business Continuity Plan and associated documentation was ongoing at the time of the audit.

An exercise is currently ongoing to define specific RTOs and RPOs for key Council systems and services.

There is a recognised need to complete a Disaster Recovery test exercise to assess/confirm the ability to recover key Council applications and systems.

The Remote and Home Working Policy requires review and updating to reflect the current processes and controls.

GOOD PRACTICE IDENTIFIED

The Council's BCP arrangements are documented as part of a Corporate Business Continuity Plan.

Backups of all Council systems and services are made and replicated to secondary site.

SCOPE

The review considered the overarching response to the Covid-19 pandemic in terms of business continuity arrangements and considered the following: the Business Continuity Plan; business impact analysis; controls over the continuation of business critical functions and resources required for this; arrangements for remote working; arrangements for making changes to working practices/staff terms and conditions, if required; communication with staff and stakeholders during period of lockdown; arrangements for identifying and promoting good practice and for sharing this with staff; lessons learnt and any remedial action taken; and monitoring and reporting arrangements.

ACTION POINTS

Urgent	Important	Routine	Operational
0	4	6	1

Assurance - Key Findings and Management Action Plan (MAP)

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
1	Directed	An exercise to review and update the Council's Business Continuity Plan and associated documentation was ongoing at the time of the audit, the last update having been completed in February 2021.	Management to complete the review and updating of Business Continuity Plan documentation and ensure it is made available to all relevant staff.	2	*Corporate BC plan taken to Apr 22 Cttee for yearly consultation and approval to go to SLT 11th May. Following SLT approval, BC plan will be updated on the Doc Centre/Grab bag/RD and communicated.* *Exercise paper going to 27th April SLT. Proposal to hold July BC exercise. Senior management to ensure all Service Level BC plans and Business Impact Assessments reviewed prior to July CHS&R Cttee and BC exercise.*	*27/05/22* *29/07/22*	*Corporate Health, Safety and Resilience Team Leader* *Corporate Health, Safety and Resilience Team Leader*
7	Delivery	There is a recognised need to complete a Disaster Recovery (DR) test exercise to assess/confirm the ability to recover key Council applications and systems. It was advised at the time of audit that management are planning to arrange a table top DR test exercise during 2022.	Disaster recovery arrangements be tested on an annual basis. Test results be documented as part of a formal test report which details test objectives, outcomes, and lessons learned. This can then be used in updating and improving the DR plan and supporting documents.	2	*A tabletop DR exercise is scheduled to take place in June.* *A test restoration of a key line-of-business system will take place in June 2022.*	*30/06/22*	*Head of Digital*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
9	Delivery	There is a recognised need to develop and introduce a program of Disaster Recovery (DR) and Business Continuity Planning (BCP) tests and drills to test the ability of the Council to maintain service in the absence of the key Council systems and services. This will include testing of particular key applications and the ability of the system owners to follow business processes and maintain services in the absence of the applications.	ICT management to liaise with business following completion of the ongoing work on reviewing the BCP and DR plans to introduce a program of DR drills testing key Council systems and applications.	2	*ICT management will liaise with the Resilience Team to develop BCP testing simulating loss of access to key Council systems.*	*29/07/22*	*Head of Digital*
4	Directed	It was noted that management was in the process of developing a staff training exercise to address IT security for remote workers at the time of the audit.	Management to develop and implement training for remote workers to address risks and security implications arising from home working including risks around physical security, awareness of unauthorised people, and the importance of regular system patches.	2	*ICT Management will work with the Information Security Team Leader to ensure that Information Security Training includes emphasis on risks associated with working remotely.*	*30/06/22*	*Head of Digital / Information Security Team Leader*
2	Directed	There is a recognised need to update the ICT Disaster Recovery Plan and associated supporting documents to reflect recent changes including the recent datacentre relocation.	ICT management to update the IT Disaster Recovery Plan and associated documents to reflect current processes and procedures,	3	*ICT management will update the IT Disaster Recovery Plan and associated documents.*	*30/06/22*	*BT*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
3	Directed	There is a Remote and Home Working Policy in place that describes the Council requirements of staff when working from home or remotely. It was noted however that this was last reviewed and updated in 2019, which was prior to start of the Covid-19 Pandemic.	Management to ensure that the Remote and Home Working Policy is reviewed and updated as necessary to reflect current home working controls.	3	*The policy has now been updated (3/5/22) and uploaded to the Council's intranet; a review of this document will take place in May 2023 or sooner as and when required.* *The Council has also recently launched a remote working guide which forms part of the new ways of working project, this guide supports and is aligned to the Remote and Home Working Policy.*	*Complete*	*Information Security Team Leader*
5	Directed	Though there are low level process documents used for reference/ training purposes it was noted that there is no documented backup policy/ process document in place to define the Council's approach to, and requirements for, backups of systems and data. A documented backup process would provide further assurance that standard practices are defined and adopted to ensure the integrity, availability, and confidentiality of Council backup data.	ICT management to ensure a backup policy is documented that reflects current backup requirements and controls. This policy should document requirements around the backup of key services, defining roles and responsibilities and required backup schedules.	3	*Documented back-up retention schedules, daily checks and over-arching system documentation are already in place.* *However, ICT Management will augment these with a back-up policy that includes roles and responsibilities.*	*30/06/22*	*Head of Digital*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
8	Delivery	It was noted that, while offsite backups of data and systems are in place, the backup solution does not currently incorporate cold/ offline backups. NCSC guidance recommends the use of cold/ offline backups to improve the security of backup data and reduce the possibility of ransomware attacks.	ICT management to consider options around the implementation of cold/offline backups to provide increased backup security.	3	*ICT Management are in the process of reviewing options for offsite/immutable back-up and have provided SLT with an initial briefing.*	*30/05/22*	*Head of Digital*
6	Delivery	While interim high level recovery point objectives (RPOs) and recovery time objectives (RTOs) have been defined, an exercise is currently ongoing to define specific RTOs and RPOs for key Council systems and services and ensure that these are given the correct level of priority from a Business Continuity Plan/Disaster Recovery perspective. The lack of specific RTO's for particular key applications/ systems increases the risk that these systems may not be recoverable within an acceptable timescale in the event of a DR scenario and where backup arrangements have been determined based on the ICT team's assessment of criticality rather than having been based on the requirements of the operational teams.	ICT to liaise with key Council management and stakeholders within the business to complete the Business Impact Assessment (BIA) of key IT systems and applications in use at the Council. Documented recovery requirements for each system should be defined and agreed between the business and ICT as part of this process.	3	*The existing RTOs and RPOs were the product of consultation with the Council's Resilience team rather than "the ICT team's assessment" in isolation.* *However, ICT Management will liaise with the Resilience Team to review services' Business Impact Assessments and ensure that the RPOs and RTOs in place for key business systems are still appropriate.*	*31/07/22*	*Head of Digital*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
10	Delivery	There were two items of evidence relating to home/ remote working arrangements that it was not possible to obtain during the timescale required for this audit. These were; • Confirmation of whether there had been a need to review/ update staff Terms & Conditions in the light of the move to home working, and; • Evidence that Display Screen Equipment (DSE) risk assessments have been completed for all required staff.	Management to satisfy themselves that any need to review/update staff terms and conditions has been addressed and that DSE assessments have been completed for all staff.	3	*The New Ways of Working scheme allows managers and staff to establish the best working practice to support our customers/business need and staff preferences. There will be a mixed approach of how staff work; hybrid, office based, homeworking etc. Existing contracts use the term – 'You will normally work at or be directed from The Forum'. HR advice is that terms and conditions will need to be amended if staff are working from home the majority of their time.* *The Council's Corporate Health & Safety management are satisfied that a robust process in place for the completion of DSEs. The latest report from Safe4work states:* *Assessments completed 496 (83%) No assessments 102 (17%).* *The system sends out invitations and reminders. Reports can be run showing staff that have/have not completed the DSE assessment and any actions. There is an expectation that there will always be a figure showing as 'no assessments' as this is live reporting taking into account new staff and leavers and time to update HR records.*	*Complete* *Complete*	*Assistant Director - People* *Corporate Health, Safety and Resilience Team Leader*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Operational - Effectiveness Matter (OEM) Action Plan

Ref	Risk Area	Finding	Suggested Action	Management Comments
1	Delivery	It was noted that the Council does not currently hold Cyber Essentials certification. It is recommended that management consider working towards this to provide further assurance around Cyber Security in the light of increased risks around Cyber Security.	ICT management should consider seeking Cyber Essentials certification.	*ICT management will review Cyber Essentials to determine if it offers any added value in combination with current commitments to meet stringent Cabinet Office standards for PSN accreditation.*

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

Findings

Directed Risk:

Failure to properly direct the service to ensure compliance with the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
GF	**Governance Framework**	There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation.	Partially in place	1, 2, & 3	-
RM	**Risk Mitigation**	The documented process aligns with the mitigating arrangements set out in the corporate risk register.	In place	-	-
C	**Compliance**	Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Partially in place	4, & 5	-

Other Findings
Formal roles and responsibilities in regard to emergency planning and business continuity are detailed as part of the Council's Business Continuity Plan and Corporate Resilience Policy Statement.
Operational and IT risk registers are maintained and reviewed on a regular basis.
Key Business Continuity Plan and Disaster Recovery documents are made available to staff via SharePoint and via physical battlebox maintained onsite for increased resilience.
Backups of Council systems and data are made as part of a daily, weekly and monthly routine

Delivery Risk:

Failure to deliver the service in an effective manner which meets the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
PM	**Performance Monitoring**	There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner.	In place	-	-
FC	**Financial Constraint**	The process operates within the agreed financial budget for the year.	In place	-	-
R	**Resilience**	Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.	Partially in place	6, 7, 8, 9 & 10	1

Other Findings
No financial issues were identified as part of this audit.
System and data backups are stored securely at a remote location.
Alerts detailing any backup failures are generated, reviewed, escalated and actioned where required.

EXPLANATORY INFORMATION

Appendix A

Scope and Limitations of the Review

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan. As set out in the Audit Charter, substantive testing is only carried out where this has been agreed with management and unless explicitly shown in the scope no such work has been performed.

Disclaimer

2. The matters raised in this report are only those that came to the attention of the auditor during the course of the review, and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Effectiveness of arrangements

3. The definitions of the effectiveness of arrangements are set out below. These are based solely upon the audit work performed, assume business as usual, and do not necessarily cover management override or exceptional circumstances.

In place	The control arrangements in place mitigate the risk from arising.
Partially in place	The control arrangements in place only partially mitigate the risk from arising.
Not in place	The control arrangements in place do not effectively mitigate the risk from arising.

Assurance Assessment

4. The definitions of the assurance assessments are:

Substantial Assurance	There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved.
Reasonable Assurance	The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved.
Limited Assurance	The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved.
No Assurance	There is a fundamental breakdown or absence of core internal controls requiring immediate action.

Acknowledgement

5. We would like to thank staff for their co-operation and assistance during the course of our work.

Release of Report

6. The table below sets out the history of this report.

Stage	Issued	Response Received
Audit Planning Memorandum:	23rd April 2021	23rd April 2021
Draft Report:	19th April 2022	3rd May 2022
Final Report:	4th May 2022	

AUDIT PLANNING MEMORANDUM

Appendix B

Client:	Dacorum Borough Council		
Review:	Business Continuity		
Type of Review:	Assurance	**Audit Lead:**	Paul Kamminga

Outline scope (per Annual Plan):	The review considers the overarching response to the Covid-19 pandemic in terms of business continuity arrangements and will consider the following: the Business Continuity Plan; business impact analysis; controls over the continuation of business critical functions and resources required for this; arrangements for remote working; arrangements for making changes to working practices/staff terms and conditions, if required; communication with staff and stakeholders during period of lockdown; arrangements for identifying and promoting good practice and for sharing this with staff; lessons learnt and any remedial action taken; and monitoring and reporting arrangements. The following key control areas will be included: • IT functions and controls regarding key information. • The existence of complete and up to date policies and processes for remote working; • The process for tracking the continuation of business critical functions to ensure they are kept up to date; • Authorisation and approval controls; • Controls to ensure the consistency across the organisation; • Processes for ensuring staff and other stakeholders are made aware of key and relevant process and procedures; • Sufficiency of staff resources for managing policies and procedures. • Exact scope to be discussed and agreed with management. • The review will also seek to share any identified good practice from similar organisations.	
Detailed scope will consider:	Directed Governance Framework: There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation. Risk Mitigation: The documented process aligns with the mitigating arrangements set out in the corporate risk register. Compliance: Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Delivery Performance monitoring: There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner. Financial constraint: The process operates with the agreed financial budget for the year. Resilience: Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.
Requested additions to scope:	(if required then please provide brief detail)	
Exclusions from scope:		

Planned Start Date:	14/04/2021	**Exit Meeting Date:**	07/04/2022	**Exit Meeting to be held with:**	Gary Osler

SELF ASSESSMENT RESPONSE

Matters over the previous 12 months relating to activity to be reviewed	Y/N (if Y then please provide brief details separately)
Has there been any reduction in the effectiveness of the internal controls due to staff absences through sickness and/or vacancies etc.?	N
Have there been any breakdowns in the internal controls resulting in disciplinary action or similar?	N
Have there been any significant changes to the process?	N
Are there any particular matters/periods of time you would like the review to consider?	N