ICT Audit

FINAL

Dacorum Borough Council

ICT Review of Network Security (Remote Access)

2021/22

August 2021

Executive Summary

OVERALL ASSESSMENT

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

PP-R04: Failures in ICT resilience or security leading to significant system downtime

KEY STRATEGIC FINDINGS

The Council has recorded an overall operational risk of IT failures. However, there is no risk register for specific ICT risks.

Generic user accounts exist for third party service suppliers. This creates an accountability risk that remote access actions are not attributable to one person.

The security posture of remote computers connecting to the Council network is not checked.

The Council was unable to confirm current users of, and approval for, audited USB devices.

GOOD PRACTICE IDENTIFIED

The Council has established IT security policies covering aspects of network access and remote working.

IT systems availability is reviewed quarterly. In the fourth quarter for 2020 - 2021 it was 100%.

SCOPE

The audit assessed the Council's IT remote working arrangements including controls that were put in place to support continued use and availability of ICT systems during the Covid-19 pandemic. The review considered remote working policies and procedures, remote working training needs, remote access rights, user authentication, password security, endpoint security and patch management of remote devices.

ACTION POINTS

Urgent	Important	Routine	Operational
0	2	5	0

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	The Council has recorded an overall operational risk of IT failures relating to system resilience and security. However, there is no risk register for individual systems and solutions. For instance, risks relating to network access should be assessed and recorded based on risks to systems and solutions which form part of this service.	The Council to establish an IT risk register to assess risks relating to systems and solutions employed in provision of network access services.	2	*We will introduce a more granular IT Risk Register for key systems and solutions.*	*29/10/21*	*Group Manager - Technology*
3	Directed	The review of the third party supplier user accounts shows the presence of six generic accounts. This creates a risk to accountability for actions carried out from these accounts as they are not attributable to a specific individual.	The Council to remove generic accounts to ensure personal accountability for actions on IT systems.	2	*These generic accounts have been deleted.*	*25/08/21*	*Group Manager - Technology*

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)
2	Directed	The Council does not have a staff training course to address IT security for remote workers.	The Council to develop a training course for remote workers to address risks and security implications arising from working in less secure environment as compared with the Council offices including physical security, awareness of the presence of unauthorised people, importance of regular system patches etc.	3	*The ICT Team will work with the Information Security Team Leader (within the Legal Governance Service) to source and provide appropriate training materials raising awareness of this increased risk.*	*30/11/21*	*Group Manager – Technology & Information Security Team Leader*
4	Directed	The review of third party user accounts identified 3 accounts which are currently enabled but have not been used for around one year. These accounts should be disabled if not in active use but still required as per the Council's IT procedures.	The third party accounts be reviewed to ensure that any accounts which are still required but are not in active use are disabled.	3	*These accounts have now been disabled and will only be re-enabled if/when actively needed.*	*25/08/21*	*Group Manager - Technology*
5	Directed	The review assessed records relating to the use and authorisation of removable media. The Council was unable to confirm current users of and approval for the tested USB devices. The audit was informed that it is likely that the tested items are older devices which have been recorded in a previous system which has since been decommissioned.	The Council to ensure that the records of current users and approvals are available for all removable data storage devices.	3	*DBC ICT will maintain records of all tested USB devices passed for approved use.*	*31/08/21*	*Group Manager - Technology*

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)
6	Delivery	The security posture of remote computers is not checked when they connect to the Council network. Therefore, computers with missing security patches or with out-of-date antimalware software may be able to connect. As a result a compromised computer may be able to join the Council network. The auditor was made aware of potentially costly solutions to address this risk.	The Council to assess and record associated risks and evaluate them against the cost of required controls.	3	*DBC ICT will prepare a short report examining this risk and the cost of mitigation to brief DBC Senior management of options.*	*30/09/21*	*Group Manager - Technology*
7	Delivery	The Council has two Microsoft Direct Access servers to provide resilience of remote access service in case one of the servers is unavailable. However, system patches are applied to both systems at the same time and without prior testing. This creates a risk that service availability may be adversely affected in case a faulty patch is applied to both systems causing them to malfunction simultaneously.	The Council to review the patching and system update process for Microsoft Direct Access servers to mitigate against the risk of both servers being unavailable.	3	*DBC ICT has made the advised change so that one Direct Access server is patched at a time, ensuring that the first server is operating satisfactorily before proceeding with the second.*	*25/08/21*	*Group Manager - Technology*

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
No Operational Effectiveness Matters were identified.				

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.	In place	-	-
RM	Risk Mitigation	The documented process aligns with the mitigating arrangements set out in the corporate risk register.	Partially in place	1, & 2	-
C	Compliance	Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Partially in place	3, 4, & 5	-

Other Findings
The Council has established the Remote and Home Working Policy and some other IT security policies covering aspects of network access and remote working.
All Council staff are required to sign up to the Council's Security and GDPR policies as part of their induction prior to being issued with a council asset.
The password policy has been established with requirements for complexity and minimum length.
The Council laptops are protected against malware and are encrypted.

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.	Partially in place	6	-
R	**Resilience**	Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.	Partially in place	7	-

Other Findings	
	IT systems availability is reviewed and a relevant record in the risk register is updated quarterly. The system availability in the fourth quarter for 2020 - 2021 was 100%.

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:	27th April 2021	27th April 2021
Draft Report:	3rd August 2021	25th August 2021
Final Report:	26th August 2021	

AUDIT PLANNING MEMORANDUM

Appendix B

Client:	Dacorum Borough Council		
Review:	ICT – Network Security (Remote Access)		
Type of Review:	Assurance	**Audit Lead:**	Andrei Tinine

Outline scope (per Annual Plan):	Risk: SR4 Rationale: Remote access is key for all organisations, new arrangements have had to be put in place, which has come about as a result of the Covid-19 pandemic. Scope: To assess the Council's IT remote working arrangements including controls that were put in place to support continued use and availability of ICT systems during the Covid-19 pandemic. The review will consider: Remote working policies and procedures; Remote working training needs have been identified and training provided to users; Remote access rights are restricted to valid and authorised users; User authentication and password security settings; Endpoint security including virus protection, WSUS and data encryption; and Patch Management of all remote devices.	
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:	01/05/2021	**Exit Meeting Date:**	19/07/2021	**Exit Meeting to be held with:**	Ben Trueman

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?	Y
Are there any particular matters/periods of time you would like the review to consider?	N