ICT Audit

FINAL

Dacorum Borough Council

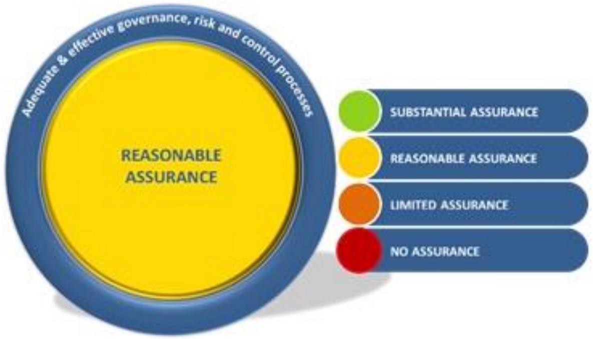
ICT Review of GDPR Information Governance

2020/21

January 2021

Executive Summary

OVERALL ASSESSMENT



ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

N/A – The risk register does not currently include a risk around compliance with GDPR. This has been raised as part of this report. : Failure to comply with the new General Data Protection Regulations could mean very substantial fines.

KEY STRATEGIC FINDINGS

There is a need for a review of the Councils e-records to ensure they are being appropriately reviewed and that a log of any destructions is retained.

Privacy notices to be drafted and published for the remaining Council service areas involved in the processing of personal data.

While the majority third party contracts have been reviewed and updated to include mandatory GDPR clauses some remain to be agreed.

The Council does not yet have a complete record of processing activity in place, although work on producing one is under way.

GOOD PRACTICE IDENTIFIED

The Council has completed significant work towards achieving compliance with the GDPR/ Data Protection Act 2018 and work on becoming fully compliant is ongoing.

GDPR / Data Protection Act 2018 training has been produced and is compulsory for all staff.

SCOPE

To review compliance with the General Data Protection Regulations (GDPR). The review will directly assess how compliant the Council is with the GDPR. This will include key elements such as (but not limited to): Privacy Impact Assessments Data Subject rights (e.g. Right to be forgotten) Data Classification and Asset management Data Security Breach Management Governance Consent Data Controllers & Processors.

ACTION POINTS

Urgent	Important	Routine	Operational
0	4	2	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)
2	Directed	There is a recognised need for an in depth of review of the Councils e-records (systems and network shares) to ensure they are being reviewed & audited to establish if they can be destroyed in accordance with the Council Retention Policy. Management advised during the audit that they were in the process of producing a plan to address this.	An exercise be undertaken to review e-records and ensure a log of any destruction is appropriately recorded.	2	*An on-going objective is to review the Council's e-records across all services to ensure that departments are aware of system records retention and any residual records on network shares. This is part of the Information Security Team Leaders (ISTL) Objectives.* *This is a major item of work, so the timetable for implementation is adjusted to reflect this.*	*30/09/21*	*Information Security Team Leader*
3	Directed	The Council has published detailed privacy notices for Council functions on its website privacy pages. It was noted that the majority but not all functions were covered at the time of audit and that work on completing the remaining notices was ongoing.	Management ensure that privacy notices are drafted and published for all Council service areas involved in the processing of personal data.	2	*There are currently 21 Privacy Policies in place. A further 6 are due to be published to ensure that every service is reflected. On ISTL Work Plan.*	*28/02/21*	*Information Security 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.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Directed	An exercise of identifying and reviewing third party contracts to ensure they include required GDPR clauses has being undertaken by the Council. While the majority of required changes have now been completed, there is a small number which are still in the process of being negotiated.	Management ensure all Council contracts and reviewed and updated to include mandatory GDPR clauses.	2	*New Clauses in place since May 2018* *Audit Note: TIAA has requested to see evidence, to verify implementation of the recommendation.*	*Completed*	*Information Security Team Leader*
6	Directed	The Council does not yet have a complete record of processing activity in place, although some work has been undertaken to produce one with work to date having focussed on the HR function. A full review of the Councils data records is planned which will enable in the production of the record of processing activity.	The record of processing activity be completed following the completion of the ongoing review of records.	2	*This work is on-going and needs a lot of dedicated time. Timetable reflects this.*	*31/12/21*	*Information Security Team Leader*
1	Directed	It was noted that, while the majority of policies have been updated to reference GDPR requirements, a number of policies require further review and updating having last been updated in 2018. These include the 'Corporate Information Security Management Policy', 'Retention Schedule Policy', 'Records Disposal' and 'GDPR UK Data Protection Act V1_2' policies.	Management to undertake an exercise to review and update all relevant information governance and security policies to ensure they are up-to-date and reflect the latest processes and controls.	3	*Retention Schedule last updated November 2020, GDPR / DPA Policy last updated November 2020. Corporate Information Security Management Policy updated 2/12/20. Records Management Policies all updated December 2020.*	*Completed*	*Information Security 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.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
5	Directed	It was noted that while the Council maintains a risk register this does not include a risk around lack of compliance with DPA/GDPR.	Management to document mitigating controls and ongoing activity around DPA/GDPR compliance as part of the Council's risk register.	3	*Operational Risk Register has been modified to include GDPR items.*	*Review by 30/04/21*	*Information Security 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
No Operational 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.	Partially in place	1, 2, 3, & 4	-
RM	**Risk Mitigation**	The documented process aligns with the mitigating arrangements set out in the corporate risk register.	Partially in place	5	-
C	**Compliance**	Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Partially in place	6	-

Other Findings

- A GDPR training course is provided with staff required to complete a quiz to demonstrate their understanding of key GDPR requirements.
- A documented Data Protection Impact Assessment process was found to be in place as required by GDPR. DPIAs should be completed in cases where new systems, services or significant changes to processes are being introduced.
- The Council has a documented process for logging and reporting data breaches and this has been reviewed and updated to comply with GDPR requirements.
- A breach log is maintained and this includes both incidents raised with the ICO and those investigated but that did not meet the criteria.
- The Council has a designated DPO in place as required by GDPR regulations. The DPO is responsible for monitoring internal compliance with data protection obligations and for overseeing the Councils data protection and GDPR controls.

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.	In place	-	-

Other Findings

Quarterly SAR reporting is produced detailing the number of SARs received and the time taken to respond. Reporting produced for Q1 2020 shows all 15 SARs were completed within the 30 day time period required by GDPR.

The Information Governance function is comprised of 1 FTE funded as part of the Finance team budget. No financial issues were identified as part of the audit.

The Councils incident response has facilitated the remote operation of the IG function during the Covid-19 pandemic.

EXPLANATORY INFORMATION

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:	14th July 2020	21st July 2020
Draft Report:	25th November 2020	22nd January 2021
Final Report:	25th January 2021	

AUDIT PLANNING MEMORANDUM

Appendix B

Client:	Dacorum Borough Council		
Review:	GDPR Information Governance		
Type of Review:	Assurance	**Audit Lead:**	Andy Shade

Outline scope (per Annual Plan):	Rationale: Failure to comply with the new General Data Protection Regulations could mean very substantial fines. An assurance audit to assess compliance with the Regulations will help to identify any weakness or omission. Scope: To review compliance with the General Data Protection Regulations (GDPR). The review will directly assess how compliant the Council is with the GDPR. This will include key elements such as (but not limited to): Privacy Impact Assessments Data Subject rights (e.g. Right to be forgotten) Data Classification and Asset management Data Security Breach Management Governance Consent Data Controllers & Processors	
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:	12/08/2020	**Exit Meeting Date:**	23/10/2020	**Exit Meeting to be held with:**	John Worts

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* GDPR/DPA 2018
Are there any particular matters/periods of time you would like the review to consider?	N