SLOUGH BOROUGH COUNCIL

Information Governance

FINAL

Internal audit report: 32.17/18

28 February 2018

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

RSM

CONTENTS

Debrief held	8 February 2018	**Internal audit team**	Daniel Harris - Head of Internal Audit
Draft report issued	14 February 2018		Chris Rising - Senior Manager
Responses received	28 February 2018		Amir Kapasi - Assistant Manager
			Zikhona Ngalo - Internal Auditor
Final report issued	28 February 2018	**Client sponsor**	Neil Wilcox - Director, Finance and Resources
		Distribution	Neil Wilcox - Director, Finance and Resources

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at http://www.icaew.com/en/members/regulations-standards-and-guidance.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Management actions raised for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is solely for the use of the persons to whom it is addressed and for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

1 EXECUTIVE SUMMARY

1.1 Background

An audit of Information Governance was undertaken as part of the annual internal audit plan for 2017/18. In December 2016, we undertook a review of the Information Governance Toolkit, for which the audit concluded that the Council could not take assurance that the controls in place to manage the risks associated with this area are suitably designed and consistently applied, with particular weaknesses identified in the design of the control framework. Within the report, a total of 2 high, 12 medium and 4 low priority management actions were agreed.

We have reviewed the medium and high priority actions agreed during this review to determine the progress made against each and to provide assurance that these actions have been fully implemented.

With the introduction of the General Data Protection Regulations in May 2018, requiring more rigorous controls, the Council need to be assured that robust information governance (IG) processes are embedded within the culture and working practices of the Council and that staff are knowledgeable of the risks of poor IG as these form the foundations of compliance with the Data Protection Act

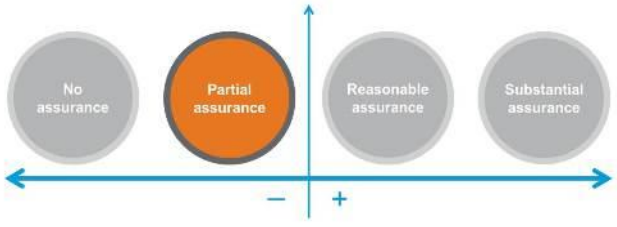
Furthermore, as the Council moves towards more collaborative working with strategic partners within the Slough economy, in particular the NHS, there is a need to demonstrate robust compliance with the Data Protection Act and GDPR requirements in relation to the security of data, whether paper based or electronic.

1.2 Conclusion

We found that while the Council had taken action to address some of the failings identified in the previous report in 2016/17, where a 'no assurance' opinion was provided, such as the commencement of mapping of data flows within the organisation, a number of issues remain. Specifically; the update of key corporate policies in relation to Information Governance, the lack of review of contracts to ensure appropriate IG clauses are included, the lack of update and monitoring of training uptake and the lack of action plans to address any of the areas identified have contributed to the partial assurance opinion.

Internal audit opinion:

Taking account of the issues identified, the Council can take partial assurance that the controls to manage this risk are suitably designed and consistently applied. Action is needed to strengthen the control framework to manage the identified risks



1.3 Key findings

The key findings from this review are as follows:

Information Governance Policy and Structure

We found that due to the restructure, and key members of staff being off sick, the Information Governance Policy still had not been updated, and consequently, the role of the SIRO had not been allocated. Lack of an up-to-date policy which is reflective of the overarching IG framework within Council and which contains sufficient guidance on IG arrangements and processes increases the risk that staff may adopt incorrect processes which are non-compliant with the Data Protection Act. This could result in data protection breaches and expose the Council to reputational risks as well as the risk of penalties from the Information Commissioner. (**High**)

While a proposed structure had been provided to demonstrate the assignment of responsibilities for Information Governance, this had not been implemented at the time of audit fieldwork due to the council restructure. Without ensuring that all IG responsibilities are formally assigned, there is a risk that these responsibilities will not be undertaken and appropriate IG arrangements and processes may not be established and embedded within the Council. (**Medium**)

Data Protection Clauses within Contracts

The Council is has still not undertaken a review of all contracts within the organisation to ensure that sufficient clauses are included to set out the Council's obligations in relation to the Data Protection Act, due to key procurement staff leaving the organisation. If the Council is unable to sufficiently assure itself that appropriate data protection clauses are contained within all contracts, and where appropriate clauses are not included; there is a risk that the Council may not be able to hold third parties to account should they be involved in a data protection breach involving Council data. The Council is also unable to evidence compliance with the toolkit requirement. (**Medium**)

Information Security Awareness Training and Specialist Training

We found issues with the monitoring and reporting of compliance with training provided by the Council, with only 590 out of 1097 members of staff having undertaken the relevant Information Security training, with limited evidence to confirm this being challenged at CMT. In addition, the Council has not identified the training needs for specialist roles such as the SIRO and Caldicott Guardian due to the current restructure. If training is not provided for specialist roles, there is a risk that specialist staff will not be trained up to an appropriate standard which could in turn lead to a breach of the Data Protection Act and the consequences associated with this. (**Medium**).

Linked to the above, we found that the Information Security Awareness training slides had not been updated to include information in relation to the Caldicott Principles, upon which compliance with the Data Protection Act is based. Where training courses do not cover all relevant areas, there is a risk of incorrect processes being followed by staff, which could potentially result in non-compliance with data protection requirements and expose the Council to the risk of penalties and reputational damage. (**Medium**)

Information Governance Action Plan

Our review identified that the Council are yet to form a suitable action plan to address gaps identified in the IG framework. It was intended to use the previous Internal Audit report as the basis for the improvement plan, however this was never formulated. The lack of a formal IG Improvement Plan to identify actions necessary to embed IG arrangements may increase the risk that staff may adopt incorrect processes which are non-compliant with the Data Protection Act. This could result in data protection breaches and expose the Council to reputational risks as well as the risk of penalties from the Information Commissioner. (**Medium**)

We found that while a process had been implemented in relation to reporting of incidents to the IG Board, this process had not been updated within the Council's Information Security Incident Reporting Policy. If the Information Security Incident Reporting Policy is not updated with the process, there will be no reference to the procedures for the reporting of and response to incidents and there is a risk that information security incidents will not be reported correctly and that may lead to incidents not being addressed. (**Medium**)

Corporate Policies and Data Protection Workplan in relation to Information Governance

No policy for the management of corporate records had been developed by the Council since the previous audit in this area. This exposes the Council to the risk of penalties due to non-compliance with the provisions of the Data Protection Act, as well as an increased risk of data breaches due to records being held indefinitely. (**Medium**)

The Data Protection and Privacy Policy, which was found to be insufficient during the previous audit, had not been updated. If the Data Protection and Privacy Policy is not updated to ensure that the roles of a Council-wide Caldicott Guardian as well as those staff responsible for supporting the Caldicott Guardian appropriately are not assigned and formally communicated, there is a risk of a lack of sufficient attention to and oversight of the work necessary to ensure the Council complies with its confidentiality and data protection obligations. (**Medium**)

No data protection annual plan had been developed since the previous audit due to a lack of resource. If the data protection work programme is not developed there is a risk that work necessary to ensure compliance to data protection and confidentiality requirements will not be identified and non-compliance may result in penalties and reputational damage. (**Medium**).

We found that while the Council had drafted a data quality policy, this had yet to be approved by the Information Governance Board, however the policy had not been updated to take account of GDPR. Without a Data Quality Policy, there is a risk of a lack of consistency as a result of controls to ensure the quality of data not having been defined. (**Medium**)

In addition, we have agreed two **'Low**' priority actions, and these are detailed in section 2 below.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Area	Control design not effective*		Non Compliance with controls*		Agreed actions		
					Low	Medium	High
Information Governance	0	(13)	13	(13)	2	10	1
Total					**2**	**10**	**1**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

.

2 DETAILED FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
Area: Information Governance								
1	**Previous Action:** The Council will review the current staffing resources in relation to information governance to ensure sufficient resources are in place to appropriately oversee information governance arrangements and responsibilities per the Health and Social Care Information Care guidance are formally assigned.	Yes	No	We were informed by the Service Lead Digital & Strategic IT that the management action to ensure staffing resources are in place to ensure and to oversee information governance arrangements and responsibilities per the Health and Social Care Information Centre guidance has been ongoing. As evidence, a draft Digital and IT team structure had been provided for our review. According to the Service Lead Digital & Strategic IT, the draft structure had been discussed with the Director of Finance and Resources (Section 151 Officer) and delays to finalise the	Medium	The Council will ensure that the draft Digital and IT team structure is approved by the IG Board and the recruitment process is undertaken to ensure that sufficient resources are in place to appropriately oversee information governance arrangements and responsibilities per the Health and Social Care Information Centre guidance are formally assigned.	. 31st July 2018	Simon Pallett - Service Lead Digital & Strategic IT

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				process had been due to the Council restructuring for senior management level that had only been finalised on 01 November 2017. Through our review of the draft Digital and IT team structure, we noted that roles such as the IG lead officer reporting to the Service Lead Digital & Strategic IT, Data Protection Officer, Freedom of Information (FOI) Officer, Records Management Officer, reporting to the IG lead officer and a FOI Support Officer reporting to the FOI Officer had been set out. We were informed that of these roles the Service Lead Digital &Strategic IT, FOI and the FOI Support were in post. In addition, we were informed that recruitment for other roles will be undertaken as soon as the structure is approved. At the time of our review, the structure had not been approved and implemented, we therefore raised an action with medium priority. Without ensuring that all IG responsibilities are formally assigned, there is a risk that these responsibilities will not be undertaken and appropriate IG arrangements and processes may not be established and embedded within the Council.				

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
2	**Previous Action** The Information Governance Policy will be reviewed and updated to ensure it reflects the arrangements and processes within the Council, in line with the HSCIC guidance, including; • roles and responsibilities, covering senior IG roles (Caldicott Guardian, SIRO and IG Lead), other key staff roles in relation to IG as well the responsibilities of the wider workforce; • the specific resources within the Council to fulfil these roles. • the key policies underpinning the overarching Information Governance Policy; • governance arrangements for overseeing the IG agenda within the Council; processes for delivering training and awareness programmes to staff; and • arrangements for reporting, escalating and monitoring IG incidents and breaches. Once updated, the policy will be presented to the IT and	Yes	No	We were informed by Service Lead Digital & Strategic IT that review of the IG Governance Policy had been added into the Council's IT Strategy Action plan dated 26 February 2017. However, no further work had been performed to ensure that the policy had been reviewed and updated as agreed in the 2016/17 internal audit report. Upon enquiry, we were informed that the Service Lead Digital & Strategic IT who was the responsible owner for the management action had been off sick and the policy review had been put on hold. We were also informed that another challenge to finalise the policy had been lack of clarity on who will take on the roles of the Caldicott Guardian and Senior Information Risk Officer (SIRO). We were also informed that following the organisational restructuring on 1 November 2017, the Caldicott Guardian role has been delegated to the Service Lead Adult Social Care Operation who is at the level of the Assistant Director. We reviewed a copy of the job description for the Service Lead Social Care Operation and confirmed that it included the Caldicott Guardian role. At the time of our follow up an individual had not been appointed to the SIRO	High	The Information Governance Policy will be reviewed and updated to sure it reflects the arrangements and processes within the Council, in line with the HSCIC guidance, including; • roles and responsibilities, covering senior IG roles (Caldicott Guardian, • SIRO and IG Lead), other key staff roles in relation to IG as well the responsibilities of the wider workforce; • the specific resources within the Council to fulfil these roles. • The key policies underpinning; • the overarching Information Governance Policy; • governance arrangements for overseeing the IG agenda within the Council; • processes for delivering training and awareness programmes to staff; and	. 31st March 2018	Simon Pallett - Service Lead Digital & Strategic IT .

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	Information Governance Board for approval, and then subsequently circulated to staff and made accessible via the intranet. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.			role, following the promotion of the Strategic Director Customer & Community Services to the role of the Interim Chief Executive. We were informed that the position of the Strategic Director Customer & Community Services has been removed from the organisational structure. In addition, we were informed that Interim Chief Executive had been continuing with the role, however, the role will need to be re-delegated. According to the discussions held, the Section 151 Officer had started chairing the meetings of the IG Board which had been the SIRO role prior to the restructuring. However there had been no formal delegation of the role to the Section 151 Officer. Lack of an up-to-date policy which is reflective of the overarching IG framework within Council and which contains sufficient guidance on IG arrangements and processes increases the risk that staff may adopt incorrect processes which are non-compliant with the Data Protection Act. This could result in data protection breaches and expose the Council to reputational risks as well as the risk of		• arrangements for reporting, escalating and monitoring IG incidents and breaches. Once updated, the policy will be presented to the IT and Information Governance Board for approval, and then subsequently circulated to staff and made accessible via the intranet. Thereafter, the policy will be reviewed annually with version control included within document to record approval and next review details.		

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				penalties from the Information Commissioner.				
3	**Previous Action** The Council will ensure that, as part of the review and re-scoping of the contracts database, fields are included for evidencing the review of contracts for appropriate clauses relating to data protection and requirements for reporting information governance incidents.	Yes	No	We were informed by the Service Lead Digital & Strategic IT that the action had been delegated to the Assistant Director of Procurement, who went on sick leave since January 2017 and officially left the Council in August 2017. The Assistant Director of Procurement vacancy has now been scrapped in the new organisational structure and the review and re-scoping of the contracts database element of the vacancy has been delegated to the Head of Procurement from 01 November 2017. We were also informed that the agreed management action will be forwarded to them for implementation as the process of reviewing the contract database had been underway. If the Council is unable to sufficiently assure itself that appropriate data protection clauses are contained within all contracts, and where appropriate clauses are not included; there is a risk that the Council may not be able to hold third parties to account should they be involved in a data protection breach involving Council data. The Council is also unable to evidence compliance with the toolkit requirement.	Medium	The Council will ensure that, as part of the review and re-scoping of the contracts database, fields are included for evidencing the review of contracts for appropriate clauses relating to data protection and requirements for reporting information governance incidents.	31st March 2018	Frederick Narmh - Head of Procurement

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
4	**Previous Action** As part of the review of training needs, the Council will ensure the inclusion of IG training as part of induction. In addition, a review will be undertaken to ensure the additional training needs of staff within specialist IG roles are identified and addressed. The training needs document will be updated to include the requirement for IG induction to be provided as part of induction, as well as the training requirements for staff within specialist IG roles.	Yes	No	We were informed that the Council has a mandatory IT training e-learning course on Information Security Awareness relating to internet security, data handling, and guidance on how data should be handled and this was available to all staff via the Intranet, along with Data Protection Awareness and the Government Connect courses. Intranet print screens and course content were provided as evidence. We were also informed that Data Protection Awareness course had not been updated and that it was to be updated in time to ensure compliance when the GDPR goes live Upon enquiry, we were informed that the Human Resources unit monitors completion of the mandatory IT training maintains a training log. The Human Resources unit submits the training log to the Corporate Management Team (CMT) monthly and non - compliance is communicated to relevant Service Leads by CMT. We reviewed the provided Information Security training report as of 6 September 2017. Through review of this report we noted that as of 6 September 2017, 590 out of 1097 members of staff had undertaken the Information Security training. We therefore reviewed CMT minutes dated 11 October 2017, however we could not confirm that the	Medium	The Data Protection Awareness training will be updated to provide guidance in line with GDPR prior to regulations going live. A review will be undertaken to ensure the additional training needs of staff within specialist IG roles are identified and the training needs document will be updated with the identified training requirements. _____ Training reports will be discussed at DMT quarterly and CMT half-yearly and details of the discussion will be recorded in the minutes.	31st March 2018 31st March 2018	Alex Cowen - IT & Business Relationship Manager Surjit Nagra- Service Lead HR

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				training report had been discussed at the CMT meeting as there had been no record made in the minutes. We were also informed by the Organisational Development Officer that CMT has requested the report format to be revised, therefore no reporting is due to be submitted until the revision of the report format is finalised in January 2018. In addition, we were provided with Data Security presentation dated 01 July 2017 that had been communicated to all staff and the presentation was also available to all staff on Insite. This includes the responsibilities of staff with regards data security and instructions over sending information by email. With regards to the ensuring the additional training needs of specialist IG roles, we were informed that the action had not been implemented, as the specialist roles had not been identified due to organisational restructuring. Through discussion we were informed that moving forward the Council intends to identify the SIRO, following which the training needs for the role will be identified and plotted for both the SIRO and the Caldicott Guardian. Now that the Caldicott Guardian has been identified, training is to be set up.				

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				If training is not provided for specialist roles, there is a risk that specialist staff will not be trained up to an appropriate standard which could in turn lead to a breach of the Data Protection Act and the consequences associated with this.				
5	**Previous Action:** The Information Security Awareness course will be reviewed and updated to ensure the content is reflective of current arrangements and includes reference to the Caldicott Principles and the processes for ensuring compliance with the Freedom of Information Act. In addition, the Council will consider merging the Information Security Awareness and Data Protection Awareness courses to provide a single course covering data protection and information governance.	Yes	No	We were informed through discussion with the IT and Business Relationship Manager, that the Information Security Awareness course has not been updated to include information with regards to the Caldicott Principles as the Caldicott Guardian role had not been delegated. In our discussions, we were informed that now that the role has been delegated, the course will be updated with the Caldicott principles and the Guardian details. Where training courses do not cover all relevant areas, there is a risk of incorrect processes being followed by staff, which could potentially result in non-compliance with data protection requirements and expose the Council to the risk of penalties and reputational damage.	Medium	The Information Security Awareness course will be reviewed and updated to ensure and includes reference to the Caldicott Principles. In addition, the Council will consider merging the Information Security Awareness and Data Protection Awareness courses to provide a single course covering data protection and information governance.	31st March 2018	Alex Cowen - IT & Business Relationship Manager
6	**Previous Action:** The Corporate IT Security Policy will be reviewed and updated to ensure it reflects	Yes	No	We were informed by the Service Lead Digital & Strategic IT that the Corporate IT Security Policy had been drafted and was due to be discussed at the Information Governance Board's next	Low	The drafted Corporate IT Security Policy will be presented to the IT and Information Governance Board for approval, upon	31st March 2018	Simon Pallett - Service Lead Digital & Strategic IT

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	the current arrangements and processes for information security within the Council. Once updated, the policy will be presented to the IT and Information Governance Board for approval, and then subsequently circulated to staff and made accessible via the intranet. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.			meeting scheduled for discussion and approval in 13 December 2017. We reviewed the draft policy and confirmed that it had been updated to reflect IT security arrangements, however it had not been updated with GDPR. Upon enquiry, we were informed that the current draft was to go to the IGB as planned, and the policy was to be updated again to ensure that it was in line with GDPR prior to regulation going live.		approval the policy will be circulated to staff and made accessible via the intranet. The Council will ensure that the policy is also updated to provide guidance in line with GDPR prior to regulations going live. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.		
7	**Previous Action:** The Council will develop and finalise the IG Improvement Plan to identify the actions necessary to embed robust IG arrangements and ensure compliance with the HSCIC IG toolkit requirements. Each action will be assigned a responsible owner and completion deadline. The plan will be reviewed and revised on an annual basis and will be subject to approval by the IT and Information Governance	Yes	No	We were informed by the Service Lead Digital & Strategic IT that the 2016/17 internal audit report actions had been used as the improvement plan with the intention to merge the internal audit actions with actions from the General Data Protection Regulation work into a formal IG Improvement Plan. At the time of our review, the formal improvement plan had not been produced. We were also informed that the improvement plan will be produced following the Digital & IT team restructuring and filling of posts. The lack of a formal IG Improvement Plan to identify actions necessary to	Medium	The Council will develop and finalise the IG Improvement Plan to identify the actions necessary to embed robust IG arrangements and ensure compliance with the HSCIC IG toolkit requirements. Each action will be assigned a responsible owner and completion deadline. The plan will be reviewed and revised on an annual basis and will be subject to	31st March 2018	Simon Pallett - Service Lead Digital & Strategic IT

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	Board. It will drive the IG agenda within the Council and progress against the plan will be monitored at each meeting of the IT and Information Governance Board, with progress updates reported to CMT periodically.			embed IG arrangements may increase the risk that staff may adopt incorrect processes which are non-compliant with the Data Protection Act. This could result in data protection breaches and expose the Council to reputational risks as well as the risk of penalties from the Information Commissioner.		approval by the IT and Information Governance Board. It will drive the IG agenda within the Council and progress against the plan will be monitored at each meeting of the IT and Information Governance Board, with progress updates reported to CMT periodically.		
8	**Previous Action:** A formalised process will be implemented for reporting, recording, investigating and managing information security incidents, which will be reflected within the Information Security Incident Reporting Policy. Once updated, the policy will be presented to the IT and Information Governance Board for approval, and then subsequently circulated to staff, made accessible via the intranet and communicated to third party providers and partner organisations. The policy will be reviewed annually thereafter, with	Yes	No	We were informed by the IT & Business Relationship Manager that data breaches were reported to the IGB at monthly meetings and they were monitored by the IGB through the IGB Action Tracker. We reviewed provided July, August and September 2017 IGB Tracker as well as IGB minutes, and confirmed that data breaches had been reported to the IGB by the IT & Business Relationship Manager. However, we were informed that the agreed management action to update the Information Security Incident Reporting Policy with the process had not been implemented. If the Information Security Incident Reporting Policy is not updated with the process, there will be no reference to	Medium	The Council will ensure that the Information Security Incident Reporting Policy is updated to reflect the reporting, recording, investigating and managing information security incidents. Once updated, the policy will be presented to the IT and Information Governance Board for approval, and then subsequently circulated to staff, made accessible via the intranet and communicated to third party providers and partner organisations.	31st March 2018	Simon Pallett - Service Lead Digital & Strategic IT

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	version control included within document to record approval and next review details.			the procedures for the reporting of and response to incidents and there is a risk that information security incidents will not be reported correctly and that may lead to incidents not being addressed.		The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.		
9	**Previous Action:** The Council will ensure that a robust framework is established and maintained for records management, including the use and monitoring of retention schedules. The Records Management Policy will subsequently be updated to reflect these processes and the responsibilities of all staff as well key staff roles in relation to records management. Once updated, the policy will be presented to the IT and IG Board for approval, and then subsequently circulated to staff and made accessible via the intranet. The policy will be reviewed annually thereafter, with version control included within	Yes	No	We were informed by the Service Lead Digital and IT Strategy that a framework for records management had been drafted however it had not been discussed with relevant services leads and therefore had not been finalised. We reviewed the policy and confirmed that it reflected these processes and the responsibilities of all staff as well key staff roles in relation to records management, however it had not been updated with GDPR. Upon enquiry, we were informed that the policy will be updated with GDPR prior to regulations going live This exposes the Council to the risk of penalties due to non-compliance with the provisions of the Data Protection Act, as well as an increased risk of data breaches due to records being held indefinitely.	Medium	The drafted Records Management Policy will be discussed with relevant service leads and finalised Once finalised, the policy will be presented to the IT and IG Board for approval. Upon approval, the policy will be circulated to staff and made accessible via the intranet. The Council will ensure that the policy is also updated to provide guidance in line with GDPR prior to regulations going live. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.	31 March 2018	Simon Pallett - Service Lead Digital & Strategic IT

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	document to record approval and next review details.							
10	**Previous Action:** The Data Protection and Privacy Policy will be reviewed and updated to ensure it details; • the requirement for the Council to have in place a Caldicott function; • the specific resources within the Council to fulfil the roles within the function, including the Caldicott Guardian, Data Protection Officer as well as those staff at directorate level with responsibility for supporting the Caldicott Guardian; • the additional training requirements for staff within the function; • the mechanisms for ensuring the effectiveness of the function, including the development and monitoring of an annual data protection work programme which identifies the work necessary to ensure the Council meets its data protection and	Yes	No	We were informed by the Service Lead Digital & Strategic IT that the agreed action to review and update the Data Protection and Privacy Policy had not been implemented due to lack of sufficient resources. We were also informed that the Council had been undertaking organisational restructuring of senior management and had therefore put staff resourcing on hold. In addition, we were informed that the recruitment process will be started and the Data protection and Privacy Policy will be updated as part of the General Data Protection Regulation work. If the Data Protection and Privacy Policy is not updated to ensure that the roles of a Council-wide Caldicott Guardian as well as those staff responsible for supporting the Caldicott Guardian appropriately are not assigned and formally communicated, there is a risk of a lack of sufficient attention to and oversight of the work necessary to ensure the Council complies with its confidentiality and data protection obligations.	Medium	The Data Protection and Privacy Policy will be reviewed and updated to ensure it details; • the requirement for the Council to have in place a Caldicott function; • the specific resources within the Council to fulfil the roles within the function, including the Caldicott Guardian, Data Protection Officer as well as those staff at directorate level with responsibility for supporting the Caldicott Guardian; • the additional training requirements for staff within the function; • the mechanisms for ensuring the effectiveness of the function, including the development and monitoring of an annual data protection work programme which identifies the work necessary to ensure the Council meets its data	31st March 2018	Simon Pallett - Service Lead Digital & Strategic IT

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	confidentiality obligations; and • the governance arrangements for monitoring the effectiveness of the function. Once updated, the policy will be presented to IGB for approval, and then subsequently circulated to staff and made accessible via the intranet. The roles will be formally assigned to the relevant staff and details published via the staff intranet. The role of Caldicott Guardian will also be communicated on the Council website. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.					protection and confidentiality obligations; and • the governance arrangements for monitoring the effectiveness of the function. Once updated, the policy will be presented to IGB for approval, and then subsequently circulated to staff and made accessible via the intranet. The roles will be formally assigned to the relevant staff and details published via the staff intranet. The role of Caldicott Guardian will also be communicated on the Council website. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.		
11	**Previous Action:** An annual data protection work programme will be	Yes	No	We were informed that an annual data protection work programme had not been developed, due to lack of resources. We were also informed that	Medium	An annual data protection work programme will be developed to identify the work necessary to ensure	31st March 2018	Simon Pallett - Service

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	developed to identify the work necessary to ensure the Council meets its data protection and confidentiality obligations. Clearly defined timescales and responsible owners will be assigned for all actions identified. The work programme will be reviewed and set on an annual basis and will be subject to approval by CMT. Progress will be monitored at each meeting of the IT and IG Board, with progress updates reported to CMT periodically.			resourcing had been put on hold during the organisational restructuring process and now that the restructuring had been finalised, recruitment of new resources will be undertaken and the annual data protection work programme will developed. If the data protection work programme is not developed there is a risk that work necessary to ensure compliance to data protection and confidentiality requirements will not be identified and non-compliance may result in penalties and reputational damage.		the Council meets its data protection and confidentiality obligations. Clearly defined timescales and responsible owners will be assigned for all actions identified. The work programme will be reviewed and set on an annual basis and will be subject to approval by CMT. Progress will be monitored at each meeting of the IT and IG Board, with progress updates reported to CMT periodically.		Lead Digital & Strategic IT
12	**Previous Action:** The Council will undertake a data flow mapping exercise to ensure all flows, both inbound and outbound, of person identifiable and sensitive information in all service areas have been identified mapped and recorded. The information flows will be risk assessed, with necessary actions identified to address risks highlighted. The outcome of the mapping exercise and the risks identified will be reviewed by the IT and Information	Yes	NA	The Council has engaged RSM UK to assist with the implementation of the action relating to the data flow exercise. At the time of our follow up, we were informed that sessions had been ongoing between SBC and RSM UK and SBC had submitted work on the data flow mapping and was awaiting on feedback.		No action raised		

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	Governance Board, prior to subsequently being reported to CMT.							
13	The Council will ensure that an Information Sharing Protocol is agreed with statutory agencies and partner organisations to govern the sharing of person identifiable and sensitive information. Information Sharing Agreements (ISA) will be subject to review and approval by the IT and IG Board prior to being entered into, to ensure they conform to the requirements of the established protocol, and these will be retained in a central repository. The agreed protocol will be communicated to all staff via the staff intranet as well as within the updated Data Protection and Privacy Policy, together with the requirement for ISAs to be approved by the IT and Information Governance Board. The agreed protocol will also be communicated on the Council website.	Yes	No	We were provided with the Information Sharing Agreement for Health and Social Care Integrated Hub dated 2016 signed by relevant partner organisations. We were informed that the approval of the ISA had been done via email, as no IGB meeting was held on 25 November 2016, due to members' absence. Email was provided as evidence of approval. We confirmed that the IS Protocol had been uploaded onto the Council's website and available to all staff. However, we were informed that the data protection policy had not been updated to include the information protocol. If the agreed Information Sharing Protocol is not included within policy, there is a risk that staff may not receive adequate guidance relating to the sharing of information which could expose the Council to the risk of reputational damage and potential penalties being imposed, if person identifiable or sensitive information is shared inappropriately.	Low	The Council will ensure that the Information Sharing Protocol is integrated into the Data Protection policy when the policy is reviewed and updated to align with GDPR. The agreed protocol will be communicated to all staff via the staff intranet as well as within the updated Data Protection and Privacy Policy, together with the requirement for ISAs to be approved by the IT and Information Governance Board. The agreed protocol will also be communicated on the Council website.	31st March 2018	Simon Pallett - Service Lead Digital & Strategic IT

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
14	**Previous Action:** A Data Quality Policy will be developed which will set out the processes and mechanisms for ensuring the quality of data used for decision-making across the Council, including the validation of data. The policy will outline the responsibilities of all staff, as well as specific, lead roles, in ensuring the quality of data. Roles will be formally assigned to staff with responsibilities for leading on data quality within the Council. Once updated, the policy will be presented to the IT and Information Governance Board for approval, and then subsequently circulated to staff and made accessible via the intranet. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.	Yes	No	We were provided with a drafted Data Quality Policy and were informed that the policy will be submitted to the Information Governance Board meeting on 13 Dec 2017 for review and approval. We reviewed the policy and confirmed that roles and responsibilities had been outlined and the processes and mechanisms ensuring the quality of data used for decision-making across the Council, including the validation of data had been set out. Through our review, we noted that the policy had not been updated in preparation for GDPR. We raised medium priority action as the policy had not been updated for GDPR and it had not approved by the IGB.	Medium	The Council will ensure that the Data Quality Policy is updated with GDPR and it is reviewed and approved by the Information Governance Board. Once approved, the policy will be circulated to staff and made accessible via the intranet. The policy will be reviewed annually thereafter, with version control included within document to record approval and next review details.	31st March 2018	Simon Pallett-Service Lead Digital & IT

APPENDIX A: SCOPE

Scope of the review

The internal audit assignment has been scoped to provide assurance on how Slough Borough Council manages the following objective:

Objective of the area under review
To ensure robust systems of control are in place to protect the Council's data.

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

In December 2016, we undertook a review of the Information Governance Toolkit and finalised the report which provided no assurance over the control framework. Within the report, a total of 2 high, 12 medium and 4 low priority management actions were agreed.

We will review the medium and high actions made as part of the previous audit and look to provide assurance that these actions have been fully implemented. These are:

- Whether there is an Information Governance Policy, which has been appropriately approved and contains the arrangements and processes within the Council, in line with the HSCIC guidance
- Whether issues with the staffing resource in relation to information governance have been addressed to appropriately oversee information governance arrangements.
- Whether there is an Information Governance Improvement Plan in place to identify the actions necessary to embed robust IG arrangements and ensure compliance with the HSCIC IG toolkit requirements. This includes whether the plan has been approved and is monitored by the IT and Information Governance Board, and reported to CMT periodically.
- Whether the Council has reviewed the contracts database to include fields for evidencing the review of contracts for appropriate clauses relating to data protection; and whether contracts have been checked to see if requirements for reporting information governance incidents have been included.
- Whether the Council includes appropriate IG training as part of the induction process, and that a training needs analysis has taken place to ensure that additional training needs of staff are identified and addressed.
- Whether the Information Security Awareness course has been reviewed and updated to ensure the content is reflective of current arrangements, and includes reference to the Caldicott principles and ensuring compliance with the FOI act.
- Whether there is a Data Protection and Privacy Policy in place which has been reviewed and formally approved and updated to include the requirements outlined in the previous report, and approved by CMT.

- Whether an annual data protection work programme has been developed and has been approved, with clear timescales and responsible owners, and whether this is approved by CMT and progress monitored through the IT and IG Board.

- Whether there is a Corporate IT Security Policy, which is regularly reviewed and reflects current arrangements and processes for information security within the Council, which has been approved by IT and IG Governance Board.

- Whether there is a formalised process for the reporting, recording, investigating and managing information security incidents and whether this has been included within the Information Security Incident Policy.

- Whether the Council has undertaken a data flow mapping exercise to ensure all flows, both inbound and outbound, of person identifiable and sensitive information in all service areas have been identified, mapped and recorded.

- Whether an Information Sharing Protocol which has been agreed with statutory agencies and partner organisations to govern the sharing of person identifiable and sensitive information.

- Whether a framework has been established and maintained for records management, including the use and monitoring of retention schedules.

- Whether a Data Quality Policy has been developed, including requirements for validation of data, the responsibilities of all staff, and whether this has been approved by the IT and IG Board

Limitations to the scope of the audit assignment:

- The review will not provide assurance that all staff have read policies and procedures, understand their responsibilities and are mitigating all IG-related risks.

- The review will not provide assurance that all actions have been implemented as the low actions will not be covered and the monitoring of the implementation of these actions are the responsibility of management.

- The review will not provide assurance that a robust framework for the security of data exists, only that the actions, which contribute to the framework, as documented above, have been implemented.

- Detailed testing may be undertaken for selected samples where appropriate and practical.

FOR FURTHER INFORMATION CONTACT

Chris Rising, Senior Manager
Chris.Rising@rsmuk.com
07768 952 380

Amir Kapasi, Assistant Manager
Amir.Kapasi@rsmuk.com
07528 970 094