



Information Sharing - SCC


Final Report




Issue Date: 04 July 2017

Working in Partnership to Deliver Audit Excellence




Executive Summary

-  This section provides an overview for senior management to understand the main conclusions of this audit review, including the opinion, significant findings and a summary of the corporate risk exposure.

Findings and Outcomes

-  This section contains the more detailed findings identified during this review for consideration by service managers. It details individual findings together with the potential risk exposure and an action plan for addressing the risk.

Appendices:

-  Audit Framework Definitions
-  Support and Distribution
-  Statement of Responsibility

Executive Summary

Overview

As part of the 2017-18 audit year SWAP was asked by the Information Governance Team at Somerset County Council to investigate and give assurance around the information sharing that takes place between the Council and its partners. As well as ensuring the required controls are in place to safeguard customer (data subject) information, assurance is needed in preparation, for the extra level of accountability that will be required in this area, for the EU-General Data Protection Regulations (GDPR) to be introduced in May 2018.

The Council currently holds 11,331 linear metres equivalent to around 37,175 boxes of dormant paper records, which equates to roughly 557,000 individual records. In addition, there are 4,166 linear metres or approximately 13,668 boxes of active paper records stored within offices.

There is no distinguishing between sensitive and non-sensitive records, but based on holdings statistics, roughly half would be 'personal' type records and an unknown percentage of these would be "sensitive".

There currently is no means of identifying quantity for active electronic records though there is approximately 500GB of storage allocated to areas that are likely to store records which may well contain personal and therefore a percentage of personally sensitive information.

These numbers of records are huge and even if only 1% contained personally sensitive material this is a lot of responsibility, a lot of risk and there could be a lot of negative impact for the Council if this information is not processed correctly.

Information Sharing can have a specific meaning being the mutual processing of information (usually personal in nature) between two or more public partners. These are usually long-standing relationships, not for profit, part of statutory duties, for the good of the individual/data subject and the responsibilities of all parties would be set out in an "Information Sharing Agreement" (ISA). An example of this would be the Council and NHS, the Council and the police or all three.

Where this information is being processed while carrying out a statutory duty, the respective partners do not need to get prior consent to process the information from the data subject. This is called a statutory gateway and precludes the need for consent. This is because the data processing is for the good of the individual and any subsequent processing must continue to be for the good of the individual not the partner agencies. The data subject does not lose their human rights concerned with data processing and nearly all the other rights under DPA and GDPR are also retained.

Relationships between these partners build up over time. The gateway allows information to be exchanged between partners before any other documentation is in place. The ISA may come a long time later when there is a long-term relationship in place which is expected to continue. The ISA may well record, for the sake of clarity, what is already happening.

Information may also be shared for non-statutory reasons and this will be shared under the controls laid out in a contract, between the two parties, as well as all relevant legislation.

The majority of the controls we are concerned with in this report are controls around the processing of personal and especially personally sensitive information. This is because if this information was processed inappropriately the impact to the data subject (mental anguish and/or discrimination) and possibly the Council (financial or reputational loss) would be that much greater.

Contracts to determine how supplier relationships are going to take place are written before the relationship starts and will make up part of a procurement exercise.

Objective

To ensure that information is shared in a way that is fair, transparent and preserves the rights of the people whose information is being shared.

Significant Findings

Finding:

The information to be processed is not one of the criteria to be used when ascertaining the “value” of a contract and therefore the level of resources to be engaged in procurement and ongoing contract management.

Although underway the Information Asset Register (IAR) is not yet complete.

Risk:

There is a risk that a low value contract involving sensitive personal data could be let and the contract may not get the sufficient level of procurement/contract management engagement. This could lead to an information security event which may then lead to loss sensitive personal data, negative impact to the data subject and subsequent negative financial and reputational loss for the Council.

There is a risk the IAR may not be delivered by May 2018 due to conflicting projects requiring similar (development) resources. This may lead to the Council not being GDPR compliant which in turn may give negative financial and or reputational impact for the Council.

Audit Opinion:

Partial

Partial - In relation to the areas reviewed and the many effective controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

All instances of personally sensitive data seem to have been identified and Information Sharing Agreements (ISA's) or Contracts put in place for the associated relationships.

Due to the public nature of the relationships in ISA's and the use of statutory gateways for compliance/permissions there is not deemed to be a high level of risk associated with any of the findings concerned with the ISA's.

On the other hand, the risks raised concerning the sharing of information within lower value contracts are significant and may go under the radar until the issue happens.

There is little documentation of the processes and there is not the necessary evidence to give a high degree of assurance that the processes are in place to update current ISA's/contracts or that new ISA's/contracts will be captured for new relationships in the future.

Well Controlled Areas of the Service

There is regular and transparent communication with partners setting out respective and mutual goals of information sharing. This along with the effective use of gateways to underpin the legalities and mandates of data sharing gives efficient use of resources in the governance of data sharing with other public bodies.

Corporate Risk Assessment			
Risks	Inherent Risk Assessment	Manager's Initial Assessment	Auditor's Assessment
1. Inappropriate sharing (or loss) of data occurs, leading to breaches of legislation which may result in financial loss or reputational damage to the authority.	High	Medium	Medium

Findings and Outcomes

Method and Scope

This audit has been undertaken using an agreed risk based approach. This means that:

- the objectives and risks are discussed and agreed with management at the outset of the audit;
- the controls established to manage risks are discussed with key staff and relevant documentation reviewed;
- these controls are evaluated to assess whether they are proportionate to the risks and evidence sought to confirm controls are operating effectively;
- at the end of the audit, findings are discussed at a close-out meeting with the main contact and suggestions for improvement are agreed.

To review the policies, processes and procedures for the sharing of personal data so an assurance can be given on the Council's current information sharing procedures and capability to respond to the dynamic threat landscape relevant to the sharing of personal data.

This audit is concentrating solely on the presence, availability and suitability of policies, processes and procedures for the sharing of personal information and especially on sensitive personal information, as this is where the greatest risk lies for both the customer (data subject) and the Council. The audit is not focussing on the current state of compliance with these frameworks.

1.1	1. Inappropriate sharing (or loss) of data occurs, leading to breaches of legislation which may result in financial loss or reputational damage to the authority.	Medium
-----	---	--------

1.1.1 Finding and Impact - Documentation of Policies Processes and Procedures

There is a full suite of Information Governance (IG) policies provided by the IG team that cover most areas of information sharing. Due to the use of automated distribution, monitoring and reporting tools there is a high level of awareness amongst officers regarding these policies.

The documentation around the inclusion and updating of contract clauses in agreements with suppliers is not embedded in a procurement and contract management system. As part of the Procurement team continuous improvement plan a contract tiering process is being introduced. Because of the concise nature of the tiering process I envisage this will be the "go to" reference document for procurement therefore it is important that IG needs are in this process. The tiering process and associated documentation does not have (personal) information mentioned as a parameter to be investigated when deciding the ongoing treatment for tendering or contract management of a contract. There is a risk that contracts (and especially low value contracts) involving sensitive personal data could be let and the contract may not get the sufficient level of procurement/contract management engagement. This could lead to an information security event which may then lead to loss sensitive personal data, negative impact to the data subject and subsequent negative financial and reputational loss for the Council.

1.1.1a	Agreed Outcome:	Priority 4
--------	-----------------	------------

It is agreed that the Service Manager for Information Governance will engage with the Strategic Manager for Procurement to discuss the inclusion of Sensitive Personal and/or Personal Data in the risk analysis that is proposed to be used for the tiering of contracts, and/or in any other current

central process that will ensure all contracts are managed in a manner commensurate with the data that is managed within the contract.

Action Plan:

Person Responsible:	Service Manager - Information Governance	Target Date:	31.03.2018
Management Response:	Initial meeting with Procurement and Legal services has already taken place. Procurement and Legal services are considering their response to make Ts & Cs within lower value contracts, containing personal data, suitably robust. No further impact on IG expected until new contract Ts and Cs are drafted.		

1.1.2 Finding and Impact - Governance of Policies Processes and Procedures

The majority of elements required can be found on most documents and I have found a satisfactory level of control in this area. There are some exceptions, in some areas, for example a policy being signed off by a lower manager than would normally be expected or perhaps a review date being missed. A verbal recommendation will be given during the close out meeting for the Service Manager Information Governance to review policy governance. The current level of governance, although not perfect, is satisfactory and does not undermine the overall the control.

1.1.3 Finding and Impact - Information Asset Register (IAR) Not Yet Complete

As the IAR is still a work in progress and is not yet nearing completion it is not yet accessible to those other than the people building it.

The aspirations regarding access are correct in that there will be a read only instance available for all officers on SharePoint/Applications Team "Excel List/Assyst and only the Information Governance (IG) plus a small team of technical/support users will have change access.

Opportunities such as the automated updating of IAR as part of the Configuration Management Process and having a plan to make a subset of the information available to the public are also being discussed, as is the use of the information already in Assyst.

I have given a number of "value added" recommendations to ICT and IG throughout this area of testing and these have been or are being pursued therefore these recommendations are not being repeated here.

The need to implement an IAR is included in the high level GDPR plan. There is though, currently no detailed project plan/roadmap covering timeframes and resources regarding the implementation of the IAR. There is a risk that the IAR may not be delivered by May 2018 due to conflicting projects requiring similar (development) resources. This may lead to the Council not being GDPR compliant which in turn may result in negative financial and/or reputational impact for the Council.

1.1.3a Agreed Outcome:

Priority 4

It is agreed that the Information Governance Officer will request project management resource to be allocated from the business change team to ensure the production of a project plan/roadmap takes place for the delivery of the Information Asset Register in the chosen area of the SCC domain. The plan will document a GDPR compliant specification of the IAR, including characteristics for each asset and exactly what is to be delivered, including time against resource to help ensure that the IAR is delivered by May 2018.

Action Plan:			
Person Responsible:	Service Manager - Information Governance	Target Date:	30.09.17
Management Response:	<p>There is a need for project management across the entire GDPR programme which the current IG team is unable to resource. Currently the IG manager does what he can between BAU.</p> <p>The specific IAR task needs to have a decision made on the right solution a) Sharepoint attached to Applications register or b) integrated to Assyst?</p> <p>A full understanding of the IAR is required well before May 2018 to facilitate other dependencies in the GDPR programme.</p>		

1.1.4	Finding and Impact _ Documentation of the ISA Process		
<p>There is an accurate list of ISA's available to those who need it. The management of ISA's takes place currently in an effective manner when needed. This is though without definitive documentation, because of the very few times when any ISA management is needed and the few people who are involved in the process.</p> <p>This lack of documentation and small number of people involved in the process means the ISA management process could be lost along with a small quorum of people meaning there would not be a continuity of process in the future and current ISA's may be lost.</p>			
1.1.4a	Agreed Outcome:	Priority 3	
<p>It is agreed that the Service Manager Information Governance will document the current ISA process and make it available (read only) along side the current ISA list.</p>			
Action Plan:			
Person Responsible:	Service Manager - Information Governance	Target Date:	31.12.2017
Management Response:	<p>There is a need for project management across the entire GDPR programme which the current IG team is unable to resource. Currently the IG manager does what he can between BAU.</p> <p>This specific task around the ISA register is important as is forms part of understanding the accountability for how information assets are created and shared. There are currently no resources in IG team to document all these Information sharing processes across all of SCC.</p> <p>Current list of ISAs is held by the Performance team in Corporate Governance.</p>		

1.1.5	Finding and Impact - Document Classification at Rest		
<p>Investigations in this audit and also general exposure to SCC documents, has shown the majority of documents not to be classified. There is a wish to implement smart storage solutions such as SharePoint which mandate the classification of documents. The programme for this is ongoing so further recommendations are not going to be given here.</p> <p>There is a culture of access controls to the areas where information is intended to be stored though there is not a culture of ensuring, through classification, these controls are duplicated in any other areas the information is subsequently processed. This means that a piece of sensitive data could</p>			

be removed from its original storage place and stored in a separate place without the appropriate controls, due to the processing officer not being aware of the content. This may lead to negative impact for the data subject(s), which if then reported lead to financial and reputational loss for the Council.

1.1.5a Proposed Outcome: Priority 3

It is agreed that the Service Manager - Information Governance will re-engage with all relevant service areas to re-assert the importance of classification of documents through ongoing awareness and training.

Action Plan:

Person Responsible:	Service Manager - Information Governance	Target Date:	31.05.2017
---------------------	---	--------------	------------

Management Response:	<p>There is a need for project management across the entire GDPR programme which the current IG team is unable to resource. Currently the IG manager does what he can between BAU.</p> <p>This specific task around a project to mark all files, folders and records within the SCC data repositories. There are currently no resources in IG team to document all these Information sharing processes across all of SCC.</p> <p>A decision needs to be made to adopt the Sharepoint approach which will roll-out to meta-data security marking to services over the coming years or to look at alternatives such as EGRESS.</p> <p>Whatever approach is decided upon this will inform the ISA task in 1.1.3 (a) above.</p>
----------------------	---

1.1.6 Finding and Impact - Document Classification in Transit

The marking (and security) of information in transit is overall well controlled. The most common way to transport information is by email and the mandating of email and attachment classification is well controlled.

The use of physical media for the transport of information is also well controlled. The classification of the items being put on to the media is not as well controlled though this will be mitigated through the previous recommendation.

There is a "block list" control for file sharing websites in place. Most tested were found to be blocked, though the availability of Google Drive, MS OneDrive (Personal not Corporate) and lifewire shows a control weakness. Information could be stored and shared outside of the County's environment and control increasing the likelihood of the information being processed in a manner contravening the rights of the data subject which in turn may lead to negative financial or reputational impact for the Council.

1.1.6a Agreed Outcome: Priority 3

It is agreed that the Service Manager for Information Governance will consult with the network support team to investigate the blocklist used for managing restricted file sharing websites and ensures that it is fit for purpose.

Action Plan:

Person Responsible:	Service Manager - Information Governance	Target Date:	30.08.2017
---------------------	---	--------------	------------

Management Response:	As this poses an imminent risk that personal data could be shared on an insecure site the IG manager will be writing to the ICT security teams to have this vulnerability looked into.
----------------------	--

Audit Framework and Definitions

Assurance Definitions

None	The areas reviewed were found to be inadequately controlled. Risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Partial	In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Reasonable	Most of the areas reviewed were found to be adequately controlled. Generally risks are well managed but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Substantial	The areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed.

Definition of Corporate Risks

Risk	Reporting Implications
High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.
Medium	Issues which should be addressed by management in their areas of responsibility.
Low	Issues of a minor nature or best practice where some improvement can be made.

Categorisation of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors, however, the definitions imply the importance.

Priority 5	Findings that are fundamental to the integrity of the unit's business processes and require the immediate attention of management.
Priority 4	Important findings that need to be resolved by management.
Priority 3	The accuracy of records is at risk and requires attention.

Priority 2 and 1 Actions will normally be reported verbally to the Service Manager.

Report Authors

This report was produced and issued by:

Fryer, Lisa, Assistant Directors
Harris, Peter, Lead Auditors

Support

We would like to record our thanks to the following individuals who supported and helped us in the delivery of this audit review:

Name, Job Title
Peter Grogan, Service Manager – Information Governance
Tony Shelbourne, Senior Business Analyst (ICT)
Andrea Binding, Corporate Records Manager
Andy Kettlety, Interim Service Manager – Service Management
Hannah Pascoe, Contract Support Officer Commercial Contract Management Team

Distribution List

This report has been distributed to the following individuals:

Richard Williams, Commercial and Business Services Director
Peter Grogan, Service Manager – Information Governance
Darren Cole, Head of ICT
Andy Kennell, Strategic Manager Operations
Dave Littlewood, Strategic Manager Information Security
Louise Day, Strategic Manager – Business Change
Martin Gerrish, Strategic Manager - Finance Governance
Gerry Cox, CEO SWAP

Working in Partnership with

Cheltenham Borough Council Sedgemoor District Council
Cotswold District Council Somerset County Council
Devon & Cornwall Police & OPCC South Somerset District Council

Dorset County Council	Taunton Deane Borough Council
Dorset Police & OPCC	West Dorset District Council
East Devon District Council	West Oxfordshire District Council
Forest of Dean District Council	West Somerset Council
Herefordshire Council	Weymouth and Portland Borough Council
Mendip District Council	Wiltshire Council
North Dorset District Council	Wiltshire Police & OPCC
Powys County Council	

Statement of Responsibility

Conformance with Professional Standards

SWAP work is completed to comply with the International Professional Practices Framework of the Institute of Internal Auditors, further guided by interpretation provided by the Public Sector Internal Auditing Standards.

SWAP Responsibility

Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.