Internal Audit Report 2018/19

GDPR and Data Sharing **18-19-12**

PAPER D

Isle of Wight Council

FINAL
May 2019

Contents

Distribution List

For action

Claire Shand, Director of Corporate Services

Helen Miles, Assistant Director Resources

Justin Thorne, Strategic Manager of Legal Services

Gavin Muncaster, Head of IT

Jonathan Murphy, Procurement and Contracts Lawyer

Debbie Downer, Strategic Manager - Organisational Intelligence

Hayley Holden, Team Leader - Procurement & Contract Monitoring

For information

Elizabeth Goodwin, Chief Internal Auditor

Executive summary (1 of 1)

Classification	Trend	By type			By scope area					
			Control design	Operating effectiveness	Total		Critical	High	Medium	Low	Advisory
No Assurance	We have not previously carried out a review with an equivalent scope	Critical	0	0	**0**	GDPR Compliance Programme	0	3	2	3	0
		High	3	0	**3**	Oversight	0	0	1	0	1
		Medium	3	0	**3**	Information Management: Follow-up	0	0	0	0	0
		Low	3	0	**3**						
		Advisory	1	0	**1**						

Total findings: 10

*** To ensure that the risk to the Council is accurately represented in this report the overall risk level is reported as 'no assurance', rather than 'critical', a change to previous practice. This more accurately represents the exposure to the Council, as Internal Audit cannot give assurance that arrangements are in place, rather than definitively concluding that they are not in place.**

Summary of findings

This review focussed on the steps the Council has taken to comply with the General Data Protection Regulation (GDPR), which became enforceable from 25th May 2018, also following up on the 2017/18 review of Information Management, rated as high risk, as below:

1. *GDPR Compliance Programme*: confirming that an appropriate programme of work has been progressed during 2018, specifically including revised governance and policies, ensuring Privacy Impact Assessments (PIAs) are completed where necessary and providing GDPR training to staff.
2. *Oversight*: confirming sufficient reporting is produced, considered by an appropriate forum.
3. *Information Management*: Follow-up: confirming that satisfactory progress is being made responding to the findings raised in the 2017/18 review of Information Management.

The overarching issue is the degree to which responsibilities for complying with GDPR are devolved to service areas and the lack of sufficient central review and quality assurance. The most significant issues relate to IT systems, contracts and Information Asset (IA) registers. Training has been provided (and completion rates are relatively good, at 86%) and there is an existing mechanism to cascade information to service areas and, in an informal way, report to the 'corporate centre'. However formal reporting is minimal, beyond training completed. There is no central record of IT systems and their GDPR 'status', limited oversight of Information Asset (IA) Registers held by service areas and, while it is known that there are a potentially large number of contracts which will need to be updated to comply with GDPR, the actual number has not been confirmed, with only 25

amended contracts agreed to date. The Council is also unusual in not having a GDPR or wider Information Management Risk on its strategic risk register - compliance is a legal requirement and until this is addressed, it represents a significant risk to the Council. Work is documented in ten detailed findings, summarised below:
Information Asset (IA) Registers: (**high risk**) IA registers are maintained at service level. Three IA registers were provided for review (Corporate Finance, IT and Adult Services). These vary in completeness and while recently updated, there are gaps on both the IT and Adult Services IA registers, for example missing asset owners. The Corporate Finance IA Register is highly likely to be out of date, last updated in April 2017. Internal Audit also notes that the IA registers provided for review use different formats. Ultimately this indicates that the Council does not have an up to date and accurate record of the information it holds and key information, for example its purpose and how it is safeguarded. There are also a number of fields (to capture information regarding each asset) missing, which are normally observed on IA Registers; for example the justification for processing personal information, who data is shared with and on what basis, for example as documented in a contract. Issues with the 'design' of the template need to be addressed, to support capturing information to comply with GDPR. Once a revised template is available this needs to be cascaded to service areas, with a central 'process' to monitor and quality assure revised IA Registers completed by service areas.

IT Systems: (**high risk**) while there has been work in service areas to upgrade IT systems to comply with GDPR, for example upgrading the Spydus system used by libraries, the Council is unusual in not maintaining and tracking the GDPR status of all IT systems centrally. Therefore, the Council does not know and cannot have any confidence that all of its IT systems and the processes on which they rely are GDPR compliant. A suitable register should be compiled, including an action to ensure GDPR compliant use of email, the GDPR status of all IT systems involving the processing of personal data assessed and any issues addressed as soon as possible, with progress formally reported to and monitored by the IGG.

Contracts: (**high risk**) revised templates, compliant with GDPR, covering both procurement and contracts were produced early in 2018 and all procurements initiated since the 1st April 2018 have used revised templates, aligned with GDPR. Work also started early in 2018 to identify which of the Council's existing contracts needed to have variations or equivalent applied to comply with GDPR. However this is a significant task and to date only 25 contracts have been updated (work to identify contracts which may need to be updated identified a potential list of 128) – until this situation is addressed the Council cannot be complaint with GDPR and work is likely to take up to the end of 2019/20 to complete. Further work is necessary, to fully risk access the scale of work necessary. This will need to be closely monitored by the Information Governance Group (IGG), to ensure that it is addressed as quickly as possible. Related to contracts some progress has been made addressing findings raised in the 2017/18 review of Information Management. However the Council is still waiting on replacement copies of 30 high value contracts (over £25,000) which the Council has misplaced and the need to hold copies of lower value contracts (under £25,000) has not yet been recommunicated to service areas; these actions should be addressed as soon as possible.

Data Protection Impact Assessments (DPIAs): (**medium risk**) revised DPIA guidance has been produced and cascaded to staff; this recommends than DPIAs are carried out whenever new projects/contracts/processes are being considered. However, Internal Audit has been informed that no DPIAs have been deemed necessary nor carried out since the 1st April 2018. In year there have been 109 procurements, at least 31 of which will have included processing of personal information. It is also likely that there will have been further new 'initiatives' initiated since the 1st April 2018 which should have triggered DPIAs. While only 'recommended' the gatekeeping of DPIAs needs to be improved. Procurement guidelines should be updated to specifically identify the need for DPIAs, while for wider 'change' the Organisational Intelligence Team (responsible for project management) should also be given a gatekeeping role.

Oversight: (**medium risk**) there are two forums, the Information Governance Group (IGG) and the Information Security Group (ISG), which oversee information management at the Council, both with agreed terms of reference, senior attendance (including the Senior Information Risk Owner (SIRO) and the Data Protection (DP) Officer), which meet regularly, with formal minutes kept. However 'formal' reporting of progress responding to GDPR is limited to training completed. Further updates have been provided verbally and minutes show discussions of actions being taken to support GDPR compliance. However there are key gaps in the reports, for example progress with IT systems and

contracts. Internal Audit also notes that there are gaps in attendees, most notably from the Procurement and Contract Management Team. Both the reporting which these forums receive and attendance need to be reviewed and addressed.

Core Documentation: (**medium risk**) the key policy related to GDPR, the Data Protection Policy, has been specifically updated to respond to GDPR. Two related policies, Protective Marking and Corporate Retention are scheduled to be reviewed; this should continue as planned. Internal Audit also notes that the link to the revised Data Protection Policy is broken on the privacy notice page on the Council's website; this should be updated accordingly. Two related findings were raised in the 2017/18 Information Management report. The first of these, to revise out of date documentation, is in progress. The second, to ensure that documentation lists the correct information management post holders, for example the Council's Senior Information Management Officer (SIRO) has not been addressed. The Council is in the process of revised information management post holders. Once this process is complete documentation should be revised accordingly.

Overall Plan: (**low risk**) the Council does not have a documented overall plan, setting out the remaining work necessary to achieve compliance with GDPR. Compiling a simple action plan, clearly capturing responsibility for actions and scheduled completion dates, will help to ensure timely progress and robust oversight by the IGG. As covered elsewhere in this report areas such as updating policies, IA registers and contracts and identifying and addressing any issues with IT system should be covered.

Record of Processing Activities (ROPA): (**low risk**) the Council's ROPA is in line with the minimum level of coverage specified in Article 30 of the GDPR. However, it is missing a number of elements, which many other organisations have included. Internal Audit is also aware that the Council has a copy of the Information Commissioner's Office (ICO) ROPA, as the result of a Freedom of Information (FOI) request. Reviewed against this there are a number of elements missing from the Council's ROPA, for example explicit links to the legislative justifications for processing, for each information asset. At a minimum the Council needs to review its current ROPA and supporting documentation against the ICO's ROPA to confirm a minimum level of sufficiency.

Data Exchange Agreements (DEAs): (**low risk**) the need to review old and potentially no longer used DEAs in our 2017/18 review of Information Management has not been addressed and is consequently re-raised in this report.

Strategic Risk Register: (**advisory**) to ensure work continues at pace and to focus minds on the actual risk to the Council represented by GDPR; consideration should be given to adding a specific risk to the strategic risk register on GDPR and managing work towards complying with GDFPR under this risk.
Narrative is included above and in detailed findings regarding further actions which are necessary stemming from the 2017/18 Information Management report. For completeness a summary of action status is provided below:

Finding	Current Position	Further Action Required
Contracts and Information Sharing	**Partially Implemented**	Continue efforts to source contracts which the Council has misplaced and remind service areas that they need to safely store copies of signed contracts. Retire redundant Data Exchange Agreements (DEAs).
Training	**Fully Implemented**	n/a
Roles and Responsibilities	**Not Implemented**	Review post holders for key information management roles, for example Senior Information Risk Owner (SIRO) and ensure the correct post holders are referenced from documentation.
High Level Documentation	**Not Implemented**	Update all information management policy documentation, most importantly the Retention Policy and Schedule.

Management Response:

The internal audit report and its recommendations for improvement are welcomed and accepted. In doing so, it is considered important to put the findings of the report into context with the wider picture of GDPR compliance and the current arrangements that are in place to deliver these new legislative requirements. We were pleased to see that recognition was given to the systems and processes that have been put in place thus far and as such are not in question as a result of this audit, other than to highlight opportunities for further improvements to be made. The council currently has only one contract lawyer and with a staffing complement of 2.6 FTEs as a corporate information unit. This is a significant reduction in capacity since 2005, in order to assist with the delivery on-going savings to meet the council's financial challenges. This approach required a devolved model of accountability for data protection compliance to individual directorates and their associated services. It is accepted that there needs to be greater corporate oversight and monitoring of compliance in order to provide assurance that the council is compliant in its legal obligations as recommended by this audit although it will be necessary to identify short term additional capacity.

The action plan that has been proposed by the Auditor, and which has been reviewed and agreed by the services affected, identifies a significant amount of work over the next 12 months in order to achieve full compliance. Whilst the council has trained the majority of its staff and is working well to minimise data breaches and to investigate and report to the Information Commissioner as required, there is other work that needs to take place across the council. In previous budget cuts, roles have been removed that would otherwise have undertaken this work. The Corporate Information Unit plays a co-ordinating role but has never been resourced to enable it to undertake the work required within the services. There has been an expectation that the services will deliver although this has never been addressed through funding. The council now has to respond to the Audit and to undertake the works identified in order to be fully compliant with GDPR. It has been identified that in order to undertake the work, which involves securing the completion of Information Asset Registers across all services, identifying the GDPR status of all IT systems, identifying all contracts over £25,000, risk rating these, updating them, recirculating guidance to all services to update contracts below £25,000, undertaking sample testing of lower value contracts, ensuring that the requirement to carry out DPIA's is met, undertaking gap analysis of the reporting to governance forums, ensuring comprehensive reporting is provided, updating the corporate Retention Policy, updating high level information management documentation, reviewing the remaining actions necessary to achieve GDPR compliance and review the current ROPA and supporting information against the ICO's ROPA; that a 12 month additional post of a document manager will be necessary. Carry forward from the underspend in Legal Services (where the Corporate Information Unit is based) is being sought so that the CIU can engage a Document Manager - who will work across the services to complete the above requirements. Without this carry forward, there is no budget to engage this post. A corporate approach in addressing this matter is considered the only way to actually achieve this as in the absence of this resource there is insufficient capacity to either deliver or monitor delivery of the required outcomes.

It is our considered opinion that despite the no assurance afforded as a result of this audit, the likelihood of the council being in breach of its duties or being at risk of action being taken is low. All necessary systems and processes for the management of data protection, reporting arrangements for breaches and the follow up management action are in place and a highly regarded, experienced and competent team of professionals, capable of providing the necessary advice and guidance form part of the central service provision.

We would like to take this opportunity to thank Isle of Wight Council staff for their help and assistance with this review.

Current year findings (1 of 10)

Information Asset (IA) Registers

Control design

1

High

Finding and root cause

Information Asset (IA) Registers are maintained at service level. Internal Audit was provided with the IA registers for Corporate Finance, IT and Adult Social Care (ASC). By far the most comprehensive is the ASC IA Register. This goes into detail regarding information assets held by the service and has been updated in the last month. The IT IA Register has also been recently updated and contains specific flags regarding the likely level of GDPR compliance. The properties of the Corporate Finance Register identify that it was last updated in April 2017 and there are a number elements which are insufficiently precise, for example 'various' for required retention periods.

IA Register formats used are different and there is minimal central oversight of IA registers. It is likely that IA registers insufficiently capture the information assets the Council holds and their current status.

The first step which needs to be taken is reviewing the fields stored against each asset, for example a number of gaps were identified regarding fields normally identified in IA Registers, which have been updated to support GDPR compliance:

- *Justification for processing*: under GDPR personal information can only be processed where there is a specific justification, for example where it is necessary for compliance with a legal obligation.
- *Retention Period*: while this information is contained in the Council's current template a number of the assets in the Finance IA Register identify this as 'various'; this is not sufficiently specific.
- *Sharing*: it is helpful to identify where information is shared internally, for example to better understand 'flows' of personal information round the Council. Where information is shared externally this field can be used to document how this is governed, for example linked to a contract or Data Exchange Agreement (DEA).
- *IT System*: this is included in the Corporate Finance IA Register but is not in a specific field; this information may not be in all IA Registers.

All IA Registers are likely to need updating. However, in advance of this requirement being cascaded, the Council should consider if the required fields need to be added to the template or that it is satisfied that it is documented elsewhere - IA Registers are often the most straightforward way to document much of this information, ensuring it is available in one place, reducing the maintenance overhead required. Specifically Internal Audit also notes that the Council's Data Retention Policy has not been updated since 2017 (as covered elsewhere in this report); once this has been updated capturing retention periods in IA Registers would be a lower overhead option than documenting it in separate retention schedules.

Once the template has been updated the need to refresh this should be communicated as a matter of urgency to service areas. At a minimum this then needs to be collated and reviewed centrally, potentially on a sample basis, to confirm its sufficiency. Progress should be reported to and monitored by the Information Governance Group (IGG).

Implications

Without an up to date register or registers of information assets, which have been quality assured the Council can neither be confident that it knows what information assets it has, nor that this information is appropriately safeguarded, specifically to support GDPR compliance.

Action plan

The Council will:

1. Review its IA Register template, to both confirm the sufficiency of required fields and identifying if adding further fields would better support GDPR compliance.
2. Cascade the updated template to service areas, with a deadline to return updated IA Registers for central review.
3. Review returned IA Registers on a sample basis, to confirm their adequacy.
4. Report progress to the IGG.

Responsible person/title

1 &2. Justin Thorne, Strategic Manager of Legal Services/IGG
3. Data processing Assistant (new role)
4. Data processing Assistant (new role)

Target date

1. July 2019
2. August 2019
3. October 2019
4. Ongoing; IA Registers to be fully updated by December 2019

Reference number

18-19-12-01

Current year findings (2 of 10)

IT Systems

Control design

2

High

Finding and root cause

There has been work carried out in areas of the Council to ensure that IT systems are GDPR compliant, most importantly that it is possible to delete data or otherwise support GDPR compliant processes. For example Internal Audit was informed that the Council's library system (Spydus) has been upgraded, to ensure it is GDPR complaint.

However, while there is some information in Information Asset (IA) registers, these are held by services. The Council is unusual in not maintaining a central register regarding the GDPR status across its system portfolio, nor reporting and monitoring this centrally. Without doing this there can be no confidence that services have ensured their systems are GDPR compliant.

The Council needs to fully identify systems which involve processing personal data, assess each system's GDPR 'status' and put a plan in place to address any issues identified as a matter of urgency. The resulting plan needs to be reported to and monitored by the Information Governance Group (IGG).

Linked to this there will be personal data contained in the Council's email system. Importantly the email system must not be used as a 'case management system', personal data must be stored in appropriate systems of record. Minutes of the Information Governance Group (IGG) do identify that this issue has been discussed, specific to Children's Services, this may have wider applicability. How the email system can be used in a GDPR compliant manner needs to be added to the register required, as identified above.

Implications

Without a central register, which clearly identifies and tracks the GDPR status of applications, the Council cannot be confident that systems are either GDPR compliant or that issues are known and an appropriate plan is in place to achieve GDPR compliance. Without these steps the Council cannot achieve GDPR compliance nor can it be confident that the information in its systems will be safeguarded, in line with the requirements of GDPR.

Action plan

The Council will:

1. Identify the current GDPR status of all systems on a central register, along with a plan as to how any issues will be addressed; this should include the email system.
2. Address issues, to be reported to and monitored by the IGG.

Responsible person/title
1. Gavin Muncaster, Head of IT/IGG 2. Data processing Assistant (new role)
Target date

1. September 2019 2. Ongoing; to be completed by December 2019
Reference number
18-19-12-02

Current year findings (3 of 10)

Contracts

Control design

3

High

Finding and root cause

The Council has taken a number of steps towards ensuring its management of contracts is GDPR complaint:

- *Standard Selection Questionnaire*: this sets out key questions to be covered during procurement processes and has been updated to respond to GDPR; all procurements initiated since the 1st April 2018 have used this revised questionnaire.
- *Revised contract terms*: contract templates have been revised to respond to GDPR, for example 'standard' contracts and more specialist templates, such as for consultancy services; these are based on good practice template, sourced primarily from the Practical Law Company (PLC), an online resource used by the Council.
- *Review of existing contracts*: contracts identified as 'potentially' involving personal data have been identified (approximately 128 letters were sent), with contractors written to using a letter template based on that recommended by Crown Commercial Services (CCS); primarily this focussed on contracts over £25,000 in value (the threshold over which contracts are overseen by the central Procurement and Contract Team).
- *Internal Enquiries*: internal emails were sent out to managers across the Council, requesting that any changes necessitated by GDPR to contracts they managed were considered, with the central team engaged with for advice/support where necessary.
- *Terms and Conditions*: standard terms and conditions for the provision of services, goods and works have all been updated on the Council's website, to respond to GDPR.
- *Advice and Support*: training provided to support GDPR compliance has covered its impact on contract and advice is provided on the Council's intranet, specifically referencing lower value (under £25,000) contracts.

The actions above were all completed between March and April 2018. During 2018 work has been ongoing, to ensure that current contracts are updated to respond to GDPR. However to date only 25 contracts have both updated to respond to GDPR and agreed with contractors, although a number are in the process of being updated – until the Council has completed updating its contract portfolio it is not complaint with GDPR requirements.

The immediate priority is to fully identify contracts over £25,000 impacted by GDPR and rate these on a risk basis. A realistic plan, with available resources, then needs to be agreed, with progress reported to and monitored by the Information Governance Group (IGG).

There is no central oversight of contracts under £25,000, as raised in previous Internal Audit reports*; responsibility for ensuring contracts below this value are GDPR compliant sits with service areas. However the Council is responsible for ensuring that service areas have responded appropriately to GDPR and further work is necessary to confirm that necessary actions have been progressed. The best way to address this is through senior management in individual services; at a high level:

- Senior management should be contacted, requesting that they identify all staff who have responsibility for any contracts, with guidance previously provided recirculated.
- Senior management should then be required to provide confirmation that appropriate variations or equivalent have been progressed.
- Sample testing should then be carried out (based on staff listings from senior management) to confirm that variations have been applied, as required.

As with contracts over £25,000 progress/status regarding lower value contracts should be reported to and monitored by the IGG.

* Findings were raised in Internal Audit's 2017/18 review of Information Management, regarding the need to locate missing higher value (over £25,000 in total value) contracts and remind service areas that they need to have copies of signed lower value contracts (less than £25,000). No guidance has been issued to service areas regarding lower risk contracts and an action is documented below regarding this issue. On higher value contract the Council still has 30 contracts it cannot find; suppliers have been contacted requesting replacement copies; this activity should continue until the Council has current copies of all its high value contracts.

Implications

If the Council has not updated contract terms to respond to GDPR then contractors may not be fully aware of GDPR requirements and personal data will be less likely to be sufficiently safeguarded, in line with the provisions of GDPR; ultimately the Council may suffer reputational damage and significant financial penalties, as specified in GDPR.

Action plan

The Council will:

1. Fully identify contracts over £25,000 impacted by GDPR, risk rate these (e.g. scale, nature of information processed etc.) and produce a plan for these to be addressed.
2. Ensure all contract over £25,000 are updated as necessary.
3. Recirculate guidance to senior managers regarding GDPR and contracts, requesting a listing of all staff with contract management responsibilities.
4. Request confirmations from senior management that variations have been applied.
5. Schedule sample testing of lower value contracts, to confirm that variations have been applied as necessary.
6. Report progress regarding revising contracts to the IGG.
7. Issue guidance to service areas that they should ensure they have copies of contracts and store these securely.

Responsible person/title
Data processing Assistant (new role)
Target date
1. August 2019 2. March 2020 3. July 2019 4. September 2019 5. December 2019 6. Ongoing, up to April 2020 7. July 2019 8. July 2019
Reference number

8. Continue activity to source replacement copies of missing high value contracts.	18-19-12-03

Current year findings (4 of 10)

Data Protection Impact Assessments (DPIAs)

Control design

4

Medium

Finding and root cause

Internal Audit has been provided with a revised Data Protection Impact Assessment (DPIA), which has been cascaded to staff and covered in GDPR training.

Internal Audit was informed that no DPIAs have been deemed necessary, nor carried out since the 1st April 2018. However 109 procurements have been initiated since 1st April 2018, at least 31 of which will involve at least some processing of personal data. There are also likely to have been further initiatives, for example IT systems, which should have triggered DPIAs.

While the Council's guidance only recommends a DPIA when 'a new project/contract/process is considered that involves the processing/sharing of personal data' (more specific guidance is referenced from GDPR, along with 'questions' to ask) it is likely that at least some of the initiatives above should have triggered a DPIA.

To 'capture' the need to consider a DPIA procurement documentation should be updated, to explicitly ask this question. This would also ensure that the need for DPIAs is considered for most new IT systems. For wider 'change' the Team best equipped to ensure this question is asked is Organisational Intelligence, the team responsible corporately for Project Management.

Implications

DPIA are a key mechanism to ensure that personal data will be protected, in line with GDPR, when new projects, contracts or processes are implemented. If this is 'missed' then noncompliance with GDPR and failure to adequately safeguard data will be more likely, opening the Council to reputational damage and significant financial penalties

Action plan

The council will assign the requirement to undertake DPIAs to the processes for procurement; project management and ICT upgrades and changes to systems to ensure that the requirement for service areas to carry out DPIAs is identified at the earliest opportunity.

Responsible person/title
Jonathan Murphy, Procurement and Contracts Lawyer Debbie Downer, Strategic Manager - Organisational Intelligence
Target date
June 2019
Reference number

18-19-12-04

Current year findings (5 of 10)

Oversight

Control design

5

Medium

Finding and root cause

There are two forums in place overseeing information management at the Council:

- *Information Governance Group (IGG)*: attended by senior staff, including the Senior Information Risk Owner (SIRO), Data Protection (DP) Officer and a range of staff representing areas across the Council, including IT and Regulatory Services.
- *Information Security Group (ISG):* attended by the SIRO, DP Officer and senior staff from IT; focussed on the 'technical' aspects of Information Management.

Both groups have recently revised terms of reference which, while not explicitly referencing GDPR, do implicitly cover this as part of wider information management. Meetings are on alternate months and formal minutes are recorded and circulated. There are two issues with these forums' oversight of GDPR:

- *Lack of comprehensive GDPR reporting*: the only 'formal' reporting on progress addressing GDPR is regarding training (this has been closely monitored, with completion rates at 86 %*). Wider reporting is limited to verbal status updates for example regarding policies being updated and two way discussions of actions required from service areas, for example reviewing their own policies and suggestions for how email can be used more securely.

  There are key areas which are missing from reporting: IT system GDPR status and progress regarding addressing issues; updating contracts to respond to GDPR; progress updating IA Registers. This is linked to the wider absence of an overall plan and all are covered more fully elsewhere in this report.
- *Attendance*: not all areas are represented. The most pressing need is for a member of the Procurement and Contract Management Team to attend, to support better oversight of addressing outstanding issues with contracts. However there may be other areas which are not currently represented, for example the Fire Service and Children's Services. Attendance should be reviewed to confirm it is adequate.

* This was incorrectly reported to the IGG as 94% due to a formula error in the completion report; this has now been corrected.

Implications

Without sufficient oversight of progress with GDPR there may be gaps in the Council's plan and progress responding to new/changed requirements may not be sufficiently timely.

Action plan	*Responsible person/title*	*Target date*	*Reference number*
The Council will: 1. Carry out a gap analysis of the reporting which goes to governance forums regarding GDPR. From this review increased reporting is required over IT systems, contracts and progress updating IA registers. 2. Once gaps in current reporting have been fully understood ensure that comprehensive reporting is provided to the forums in future, until GDPR becomes 'business as usual'. 3. Review the current attendance at the IGG; at a minimum there needs to be some representation from the Procurement and Contract Management Team, although there may be further areas which are not adequately represented.	1. Data processing Assistant (new role) 2. Justin Thorne, Strategic Manager of Legal Services 3. 2.Justin Thorne, Strategic Manager of Legal Services	1. July 2019 2. August 2019 3. Ongoing	18-19-12-05

Current year findings (6 of 10)

Core Documentation

Control design

6

Medium

Finding and root cause

Internal Audit was provided with:

- 2018 Data Protection Policy
- 2016 Protective Marking Policy
- 2017 IWC Corporate Retention Policy

The key GDPR policy is the Data Protection Policy which has been updated. However, the second two documents above need to be updated, to respond to GDPR requirements. Regarding the first policy it was noted that the link to this Policy is does not work from the privacy notice page on the Council's website; the link should be updated, to point to the new Policy.

For context two related findings were raised in the 2017/18 Information Management report:

- To review and update high level documentation; as above this has been partially addressed.
- To review the post holders for key information management roles, for example the Senior Information Risk Owner (SIRO); the 2017/18 report identified that the high level documentation listed post holders which were a number of years out of date. The Council is in the process of reallocating these roles, for example the SIRO; once this process is complete high level documentation should be updated accordingly.

Implications

If core policies have not been updated and are out of date, then staff may be given incorrect guidance regarding how to comply with GDPR and wider Information Management, consequently failing to follow good practice.
If links to policy information do not work then residents/website users will not be able to confirm the Council's arrangements and how their personal information is being safeguarded.

Action plan

1. The Council will update, cascade and promote to staff:

- The 2016 Protective Marking Policy
- The 2017 IWC Corporate Retention Policy

Responsible person/title
1 & 2. Justin Thorne, Strategic Manager of Legal Services 3. Data processing Assistant (new role)
Target date

2. Ensure the broken link to the 2018 Data Protection Policy on the Council's website is corrected. 3. Ensure that high level information management documentation is updated to identify the correct post holder for information management roles, for example the SIRO.	1. January 2020 2. Completed 3. July 2019
	Reference number
	18-19-12-06

Current year findings (7 of 10)

Overall Plan

Control design

7

Low

Finding and root cause

There is no overall plan to manage the Council approach to addressing GDPR requirements. While there is oversight from the Information Governance Group (IGG) it would be helpful to compile a simple action plan, with assigned ownership and due dates, for the key steps outstanding to enable the Council to comply with GDPR in a timely manner. From this review, as covered in more detail elsewhere in this report, the most important actions which need to be taken are:

- Reviewing and updating core policies to respond to GDPR; these should be individually identified.
- Ensuring that all GDPR issues regarding IT systems, including email, are understood and there is a clear plan to address them.
- Updating and quality assuring Information Asset (IA) Registers.
- Ensuring that scale of the work necessary to update contracts is understood and there is a clear plan to update them.

The last three above will require separate action plans in their own right, as covered elsewhere in this report. However an overarching plan would help to provide an overview of progress and assist robust monitoring by the Information Governance Group (IGG). This would also demonstrate the Council's commitment to addressing the requirements of the GDPR legislation.

Implications

Without an overarching plan it will be more difficult to monitor progress across the portfolio of activities necessary to achieve compliance with GDPR; progress may be less timely and potentially activities may be missed.

Action plan

The Council will:

1. Review the remaining actions necessary to achieve GDPR compliance, assign ownership, agree completion dates and document this on an appropriate action plan.
2. Report progress to the IGG.

Responsible person/title
Data processing Assistant (new role)
Target date
1. July 2019 2. Ongoing; to be completed by March 2020
Reference number
18-19-12-07

Current year findings (8 of 10)

Record of Processing Activities (ROPA)

Control design

8

Low

Finding and root cause

The Council has a Record of Processing Activities (ROPA), which contains the minimum necessary level of information specified in Article 30 of the GDPR. What is 'good practice' regarding the content of ROPAs is still evolving, with some organisations choosing to contain detailed information regarding each asset, for example specific legislative justifications for processing each asset and specific retention periods for each asset. However these may be easier for organisations to hold elsewhere, for example in IA registers (as suggested elsewhere in this report) or in standalone retention schedules.

Internal Audit is also aware that the Council has received a copy of the Information Commissioner's Office (ICO) ROPA, as the result of a Freedom of Information (FOI) request. This is more detailed than the version currently in place at the Council. For example all information assets are separately listed, with details of why each is required and links to both the 2018 Data Protection Act and GDPR, regarding the justification for processing. However the Council chooses to proceed at a minimum the Council's current ROPA and related information repositories need to be reviewed against the ICO's ROPA, to ensure they meet a minimum level of sufficiency.

Implications

If the Council's ROPA and supporting documentation do not meet a minimum level of sufficiency expected then the Council is not complying with GDPR. Ultimately this could lead to regulatory fines and reputational damage to the Council. At a more granular level it is less likely that sensitive personal data will be adequately safeguarded.

Action plan

The Council will:

- Review its current ROPA and supporting information against the ICO's ROPA, to ensure it meets a minimum level of sufficiency.

Responsible person/title
Data processing Assistant (new role)
Target date
October 2019
Reference number
18-19-12-08

Current year findings (9 of 10)

Data Exchange Agreements (DEAs)

Control design

9

Low

Finding and root cause

When information is 'shared' detail covering, for example, what is shared, who it shared with, for what purpose, how long it will be retained and what safeguard will apply need to be agreed and documented. Often this will be captured in contracts or equivalent. However, where this is not the case, usual practice is to document this in a Data Exchange Agreement (DEA).

As agreed in the 2017/18 Information Management report a revised Data Sharing Template has been produced by the Council and the need to retire redundant DEAs has been highlighted to service areas. However, while no overall listing is available, a number of clearly out of date (2010 and before) DEAs remain on the Council's intranet. Through the IGG this issue needs to be highlighted to service areas, with all out of date DEAs removed as possible, ideally by June 2019.

Implications

If, where data is shared, the purpose of sharing and what safeguards will be applied is not clearly documented then personal data may not be appropriately safeguarded, increasing the likelihood that it will be comprised, leading to reputational damage and financial penalties to the Council.

Action plan

The Council will:

- Ensure all redundant DEAs are removed from the Council's intranet.

Responsible person/title
Vanda Niemiec, Senior Information Management Officer
Target date
Completed
Reference number
18-19-12-09

Current year findings (10 of 10)

Strategic Risk Register

Control design

10

Advisory

Finding and root cause

The Council is unusual in having neither a specific risk regarding GDPR on its strategic risk register nor a wider risk on Information Management. Given the Council's current position regarding GDPR compliance and the scale of work necessary until it can have confidence that it is GDPR compliant managing the work necessary under a strategic risk should be considered. This would both help to ensure this is assigned an appropriately high priority and focus minds on the actual risk to the Council represented by the current position.

Recommendation

Add GDPR to the strategic risk register or equivalent, managing remedial work under this strategic risk.

Appendix A: Basis of our classifications

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Critical	A finding that could result in a: • Major loss of service, including several important areas of service and /or protracted period. Service Disruption 5+ Days	A finding that could result in: • Adverse and persistent national media coverage • Adverse central government response, involving (threat of) removal of delegated powers • Officer(s) and/or Members forced to resign	A finding that could results in: • Death of an individual or several people	A finding that could result in: All personal details compromised/ revealed	A finding that could result in: • Litigation/claims/ fines from Department £250k + • Corporate £500k +	A finding that could result in: • Costs over £500,000	A finding that could result in: • Complete failure of project/ extreme delay – 3 months or more
High	A finding that could result in a: • Complete loss of an important service area for a short period • Major effect to services in one or more areas for a period of weeks Service Disruption 3-5 Days	A finding that could result in: • Adverse publicity in professional/municipal press, affecting perception/standing in professional/local government community • Adverse local publicity of a major and persistent nature	A finding that could result in: • Major injury to an individual or several people	A finding that could result in: Many individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from • Department£50k to £125k • Corporate £100k to £250k	A finding that could result in: • Costs between £50,000 and £500,000	A finding that could result in: • Significant impact on project or most of expected benefits fail/ major delay – 2-3 months

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Medium	A finding that could result in a: • Major effect to an important service area for a short period • Adverse effect to services in one or more areas for a period of weeks Service Disruption 2-3 Days	A finding that could result in: • Adverse local publicity /local public opinion aware • Statutory prosecution of a non-serious nature	A finding that could result in: • Severe injury to an individual or several people	A finding that could result in: • Some individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £25k to £50k • Corporate £50k to £100k	A finding that could result in: • Costs between £5,000 and £50,000	A finding that could result in: • Adverse effect on project/ significant slippage – 3 weeks–2 months
Low	A finding that could result in a: • Brief disruption of important service area • Significant effect to non-crucial service area Service Disruption 1 Day	A finding that could result in: • Contained within section/Unit or Directorate • Complaint from individual/small group, of arguable merit	A finding that could result in: • Minor injury or discomfort to an individual or several people	A finding that could result in: • Isolated individual personal detail compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £12k to £25k • Corporate £25k to £50k	A finding that could result in: • Costs less than £5,000	A finding that could result in: • Minimal impact to project/ slight delay less than 2 weeks
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.						

Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	*Points*
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification		*Points*
	Low	6 points or less
	Medium	7– 15 points
	High	16– 39 points
	Critical	40 points and over

Appendix B: Terms of reference

Background and Scope

The General Data Protection Regulation (GDPR) was adopted on 14th April 2016, became enforceable from 25th May 2018. GDPR builds on and replaces the previous legislation applicable to personal information, the Data Protection Directive. While both have the same overarching aim, to ensure that personal information is adequately safeguarded, GDPR introduces new rights, for example the right to be 'forgotten' and most importantly a more robust sanction regime for breaches, specifically fines of up to €20 million or 4% of the annual worldwide turnover of the preceding financial year for an organisation.

The Isle of Wight Council has responded comprehensively to GDPR, with a programme of work in progress covering revised policies as necessary, providing training to staff and carrying out Privacy Impact Assessments (PIAs), to ensure that all personal information is 'known', with appropriate safeguards planned for.

This audit follows on from Internal Audit's previous review of Information Management and includes a specific sub-process to confirm that satisfactory progress is being made to address issues reported in the 2017/18 Information Management review. Regarding GDPR this audit will not review the Council's arrangements against GDPR, rather the focus of this review will be on the work the Council has carried out, the aim being to confirm that satisfactory progress is being made and appropriate oversight is in place, with any issues escalated to senior management so they are correctly informed regarding the Council's position regarding GDPR.

While our work is designed to help the Council address your obligations under the Regulations, you remain responsible for ensuring compliance with your legal obligations, including the design, implementation, operation and oversight of appropriate systems to achieve ongoing compliance. Our work is not the only factor you should take into account when assessing your compliance and does not guarantee that the Council is fully compliant with the GDPR.

You appreciate that in many instances regulatory issues also have legal implications. In these cases legal advice on definitions and interpretations may be necessary. This review does not include the provision of legal advice and we make no representations concerning questions of legal interpretation.

The sub-processes, control objectives and potential related risks included in this review are:

#	Control objective	Potential risks	Summary of Fieldwork
1	**GDPR Compliance Programme** The Council has an appropriate programme of work to ensure GDPR compliance including: • Revising policies and information management roles, to align with GDPR. • Implementing a programme of training, to ensure Council staff have the skills to support GDPR compliance.	If the Council is not taking appropriate steps to ensure compliance with GDPR then personal data will be more likely not to be adequately safeguarded, ultimately leading to the Council suffering significant regulatory fines; at a more granular level: • If policies and roles are not revised to align with GDPR then expectations may be unclear and there may not be appropriate corporate functions to support and ensure compliance with GDPR.	On a sample basis internal audit will confirm: • Policies and role definitions have been reviewed to identify changes necessitated by GDPR and revised as necessary. • A programme of GDPR training has been designed, the relevant audience has been identified and progress regarding training completion is on track with schedule. • Processes and systems have been reviewed to identify where PIAs are necessary, progress carrying out PIAs and any necessary actions identified as a result are on track with schedule.

#	Control objective	Potential risks	Summary of Fieldwork
	• Carrying out Privacy Impact Assessments (PIAs) to identify where GDPR is applicable, with appropriate follow-up actions taken. Progress is on track with projections.	• If training is not provided then staff will be less likely to have the knowledge/skills to ensure GDPR compliance. If PIAs are not carried out then the Council may not have fully identified and carried out the actions necessary to safeguard personal data and ensure compliance with GDPR.	
2	**Oversight** Regular reports are produced, showing detailed progress regarding the Council's GDPR compliance programme. Reports are considered by appropriate forums, with summary/exception information escalated as necessary.	If sufficient reporting, monitoring and escalation arrangements are not in place then senior management may have an inaccurate view of the Council's progress towards ensuring GDPR compliance; any issues will be less likely to be identified and addressed at the earliest opportunity. GDPR breaches could have significant reputational and financial impact on the Council.	On a sample basis internal audit will confirm: • Regular reports are being produced, which clearly summarise the progress being made implementing the GDPR compliance programme and any issues/delays which have been encountered. • Reports are being considered by forums with an appropriate membership, which meet regularly and escalate any issues to senior management.
3	**Information Management: Follow-up** Satisfactory progress is being made implementing actions agreed in response to internal audit's 2017/18 review of information management: • Actions which have reached their scheduled implementation dates have either been implemented, or delays have been agreed by an appropriate authority, with revised implementation dates agreed. • Appropriate progress is being made on actions which have not yet reached their scheduled implementation dates.	If actions stemming from internal audit reviews are not implemented in a timely manner then risks the actions aim to mitigate will remain unaddressed.	Internal audit will review evidence provided to confirm, as appropriate: • Actions have been satisfactorily implemented. • Actions have been rescheduled. • Satisfactory progress is being made towards implementing actions.

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulation or other changes; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.