























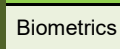
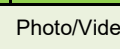
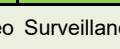

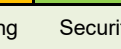


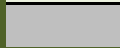










# Information Governance Audit

## 1. Summary Findings

<b>Organisation:</b>		<b>Overall Opinion</b>	<b>Adequate Assurance</b>		<b>Direction of Travel</b>	<b>Higher compliance</b>						
<b>Essex County Fire &amp; Rescue Service</b>		<b>Audit Sponsor:</b>	Hope Osayande		<b>Report Issued</b>	13/09/2019						
<b>Risk Management</b>												
<b>Risk Ref</b>	<b>Risk Area</b>					<b>Impact</b>	<b>Likelihood</b>	<b>Rating</b>				
1	<i>Immature information governance cannot effectively evidence current practices to the regulator</i> Regulator would interpret as systemic failing and would increase likelihood of high monetary penalty in the event of scrutiny					Critical	Minor					
2	<i>Organisation data is lost/processed in a non-compliant manner due to gaps in policy and processes</i> Deriving from vulnerabilities in mover/ leaver processes, device management and access from personal devices					Major	Moderate					
3	<i>Breach of Information Governance policies due to lack of awareness, communication and training</i> Where employee education needs are not effectively analysed and met, practice will not be compliant with policy					Moderate	Moderate					
4	<i>Organisation data is shared inappropriately/ illegally due to insufficient understanding of legislation</i> Insufficient knowledge to develop effective sharing process, supporting the disclosure of data through legally legitimised routes					Moderate	Minor					
5	<i>Suppliers breach information legislation through lack of contractual controls</i> Deriving from lack of clarity on compliance expectations in contracts and agreements and ineffective controls over third party access					Moderate	Minor					
<b>Summary Findings</b>		<b>Audit Areas Overview:</b>				<b>Colour Key</b>						
<p>There are a number of positive areas of compliance, such as the Authority's handling of statutory requests; security incident process; staff training; CCTV; and the completion of the Records of Processing Activity (ROPA), which has been completed but usability will be enhanced by the use of a new database which staff are currently in the process of populating. The Authority should now ensure compliance is fully met in the following areas: clarification on roles and responsibilities; ensuring all policies are complete and available to staff; privacy notices are fully compliant and the DP Policy Statement is available online; the security measures document is completed as evidence of your compliance; and non-disclosure agreements are completed by relevant individuals. Once this work has been completed you will have placed yourself in the best position to defend any complaints or concerns raised by the public or the</p>		Roles	Policy	Reporting	Notification	Assets		Critical priority issues identified				
									Major priority issues identified			
		Flows	Training	Retention	Risk	Suppliers		Moderate priority issues identified				
									No / Minor Issues identified			
		Requests	Incidents	Assessment	Notices	Consent		Not assessed as part of this audit by request or not applicable				
												
Biometrics	Photo/Video	Surveillance	Marketing	Security								
												
						 						

2. Audit Findings:

# 1. Basic Evidence Pack

Previous	Audit Area	Findings	New	Risk
<b>A. Roles:</b>				
	1) A Data Protection Officer is in place with a documented Contract	In Place		1,2,3,4,5
	2) A Senior Information Risk Owner is in place with a documented role description	Partially in Place (In progress)		
	3) A group which makes decisions on Data Protection issues has their remit documented in their Terms of Reference (e.g. Senior Leadership Team)	Not in Place (No progress)		
Comments	<i>Tracy acts as the SIRO, but she is not on the Board or SLT, and there is no role description. Reporting is done on a monthly basis, which also feeds into 1/4rly reports for SLT, but there is nothing within their TOR to show their responsibilities.</i>			
<b>B. Assets &amp; Flows:</b>				
	1) The Information Asset Register is complete	In Place		1,3,4,5
	2) The Data Flow Register is complete	In Place		
	3) Legal Conditions are identified against all Data Flows	In Place		
Comments	<i>Assets and flows complete for separate departments. Currently transferring assets and flows to a new system DPOrganizer</i>			
<b>C. Security:</b>				
	1) There is a general description of 'Technical Security' in a Security Measures document	Not in Place (No progress)		1,2,4,5
	2) There is an appropriate general description of 'Organisational Security' in a Security Measures document	Not in Place (No progress)		
	3) Issues identified with current security measures are formally recorded as risks	In Place		
Comments	<i>Have had talks with IT regarding technical security in place; suggested complete security measures for evidence</i>			
<b>D. Retention:</b>				
	1) A comprehensive Retention Schedule is in place	In Place		1,2
	2) Decisions on changes to retention rules have been recorded	In Place		
	3) Data is structured in a way that supports effective management of retention	Partially in Place (In progress)		
	4) Electronic systems functionality supports compliance with retention policy	In Place		

Comments	<i>In built into CRM, ERB etc. Staff switched on. However, W drive, kept as bin! Everyone dumps stuff in there, decluttering takes place periodically. More problems occur with hardcopy papers out at station offices</i>			
----------	--	--	--	--

### E. Privacy Notices:

	1) Identify which Privacy Notices are relevant to the Organisation, review and publish	Partially in Place (In progress)		1,3,4
	2) Publish a Data Protection Policy Statement where the organisation processes a high volume of special category data	Not in Place (No progress)		
	3) Review the forms you use to obtain data ensuring you provide links to the right Privacy Notice for the type of data you're asking for.	Not in Place (No progress)		

Comments	<i>Retention needs to be added to PNs. Need to add privacy statement to forms completed for home safety visits.</i>			
----------	---	--	--	--

### F. Policies:

	1) Ensure all relevant Information Governance policies are in place and made available to staff	Partially in Place (In progress)		1,2
	2) Make policies available to employees through your normal policy awareness processes	Partially in Place (In progress)		
	3) Publish the Data Protection and Statutory Requests policies on the website in the same location as your other policies	Not in Place (No progress)		

Comments	<i>Staff told in various ways - weekly briefing, online system etc, but policies not readily available following this. DP policy is very long - could review to see if it could be more user friendly. Need to ensure other IG policies are completed.</i>			
----------	--	--	--	--

### G. Suppliers:

	1) Data Processors are identified	In Place		1,3,4,5
	2) An evidence file/ folder is established containing the 'Controls' you have over your Processors (contract/ agreement/ Terms & conditions, their Privacy Policy etc)	In Place		
	3) These Controls have been reviewed to decide whether they are sufficient	In Place		
	4) Processors for whom you have insufficient evidence have been contacted requesting additional assurances and their responses reviewed and retained	In Place		

Comments	<i>Procurement team handled this. Gave them GDPR assurance forms to send out to all 3rd party processors. Dealt with some smaller ("one man band") companies separately.</i>			
----------	--	--	--	--

### H. ICO Register:

	1) There is a current entry on the ICO's Register of Data Controllers (ICO website)	In Place		1
--	---	----------	--	---

### I. Training & Awareness:

	1) Organisation employees have been briefed on GDPR changes	Partially in Place (In progress)		1 2 3 4
	2) Identify training needs across the various staff roles within the organisation	In Place		
	3) Staff handbook has been updated to include a detailed induction checklist making	In Place		

	explicit reference to relevant policies, procedures and guidance	In Place		1,4,5,7
	4) Training records are retained as evidence of training activities	In Place		
	5) Make information available to public to raise awareness over their rights	In Place		
Comments	<i>Have done numerous courses for different roles eg Act Now did courses on Surveillance for managers and IAOs. IGS doing IAO next week. Hope attends team meetings, and delivers induction sessions. eLearning should have been done by everyone, use Kent F&amp;R eLearning platform, and know 61% of staff have completed it, but they can't find out who has not completed. Need to contact KFR direct.</i>			

## 2. Activity Management

Previous	Audit Area	Findings	New	Risk
<b>A. Impact Assessment:</b>				
	1) Adopt a process for managing Impact Assessments	In Place		
	2) Identify (on your Information Asset Register) the assets which will require Impact Assessments if there is a change to the way you manage that data in the future	In Place		
	3) Identify the individual who will conduct Data Protection Impact Assessments and liaise with the DPO over approval	In Place		1,2,4,5
	4) Make sure that employees who have the authority to buy software or engage suppliers are aware of the need to consult the individual who conducts Impact	Partially in Place (In progress)		
Comments	<i>Project owners know to do it. Some departments still miss it</i>			
<b>B. Security Incidents:</b>				
	1) Adopt a process for managing security incidents to include roles and responsibilities and timescales.	In Place		
	2) Ensure that the definition of a security incident is agreed and made known to employees	In Place		1,2,3,4,5
	3) Maintain a record of security incident investigations and lessons learned	In Place		
Comments	<i>Have an online form for staff to complete for data breaches. 2 have been reported to the ICO. Lessons learned used in training, Many processes have changed as a result of Security Incidents.</i>			
<b>C. Procurement:</b>				
	1) Identify the individual / team who will ensure that Data Protection procurement risks are identified and decide on the appropriate 'controls' over the supplier	In Place		
	3) Data Protection assurances obtained from successful bidders are held on a Supplier Evidence file	In Place		1,3,4,5

D. Sharing:				
	1) Use the Records of Processing Activity (ROPA) spreadsheet, Data Flow Mapping (DFM) tab to identify who the Organisation shares data with	In Place		1,3,4,5
	2) Use the ROPA spreadsheet to identify why you are allowed to share data in this way (identifying the legal conditions and any sharing agreements)	In Place		
	3) Use the ROPA spreadsheet to explain how data should be shared securely	In Place		
	4) Ensure the bodies you share data with are described on Privacy Notices	In Place		
	5) Ensure there is a process for getting the advice of the DPO whenever there is a request to share data with a body not already captured on the ROPA record	In Place		

E. Non-Disclosure:				
	1) Identify any individuals who are allowed access to personal data, who aren't employed by the organisation or by a contractor (e.g. Volunteers)	In Place		1,3,4,5
	2) Ensure these individuals sign Non-Disclosure Agreements and that these records are kept in line with your retention periods for staff	Partially in Place (In progress)		
	3) Ensure that the process for approving such individuals to work in the organisation in the future requires an 'NDA' to be signed and retained	Partially in Place (In progress)		
Comments	<i>Volunteers read DP policy, and DP mentioned on application process. Could add something to this about non disclosure. Procurement use NDAs, but this is mainly for organisations. Suggested using our NDAs for individuals in future.</i>			

F. Rights:				
	1) Ensure staff are aware of how to recognise requests and complaints under GDPR rights and direct the request to an individual responsible for co-ordinating with the DPO	In Place		1,3,4
	2) Ensure that there is a process to record requests, and advise the DPO as soon as possible	In Place		
	3) Ensure that there is a clear process to approve suggested responses received from the DPO, respond to them and record them	In Place		
Comments	<i>Excellent system in place. IGS did SAR training session in April. Achieving 97% for FOIs/EIRs and similar for SARs</i>			

### 3. Review

Previous	Audit Area	Findings	New	Risk
----------	------------	----------	-----	------

A. Reporting:				
	1) Decide on what GDPR performance data you wish to report to the appropriate decision-making body within your existing annual reporting process. How frequently?	In Place		

2) Data is being recorded on:	Security Incidents	In Place	1,3
	Freedom of Information Requests/EIR	In Place	
	Subject Access Requests	In Place	
	Training & Awareness	In Place	
	IT Account Management	Not in Place (No progress)	
	Assets & Data Flows Reviews	In Place	
	Records Management Activity	In Place	
	Surveillance Reviews	In Place	
	Privacy Impact Assessments	In Place	
	Data Audits	In Place	
3) Ensure that those responsible for recording this information are aware of the reporting requirements and when the data will be required	In Place		
Comments	Weekly reporting done for SLT with full 1/4rly reports. Only area not covered is IT		
<b>B. Policy:</b>			
1) Annual reviews of Policies which are relevant to GDPR compliance are taking place, including amendment and approval. Who are these owned by (eg previous audit recommended Performance and Data Team)	In Place	1,2	
	2) Reviews are recorded on the Policy Change log		Not in Place (No progress)
<b>C. Risk:</b>			
1) Data Protection risks are reviewed, rated and controls are recorded	In Place	1,2,3	
<b>D. Contracts:</b>			
1) Undertake an annual review of Data Processors to ensure the services are being delivered in a compliant manner and that there is sufficient documentation in place to explain how the service is delivered (consider Brexit)	In Place	1,3,4,5	
Comments	A big review took place following GDPR. Already considered Brexit implications in March, satisfied they are OK		
<b>E. Training:</b>			
1) The effectiveness of information governance training is reviewed, using staff feedback and analysing the nature and frequency of security incidents	In Place	1,2,3,4	
<b>F. Surveillance:</b>			
1) Undertake an annual review of CCTV cameras and use the CCTV register to assess			

	1) Undertake an annual review of CCTV cameras and use the CCTV register to assess and confirm whether you are satisfied that the continued use of CCTV is necessary. Include any other surveillance equipment body worn camers, ANPR, drones. Consider retention of images. Is signage in place. Included in privacy notice. (signage = layer 1: INC. DC, purpose, DPO, contact to exercise rights, weblink to full notice; layer 2 = full privacy notice on website covering use of surveillance. On dash and back of truck	In Place		1,2,3,4,5
Comments	CCTV (all surveillance) has been a major focus for Hope. Worked on signage in buildings and fleet vehicles to ensure correct. Training has been delivered to relevant staff. New processes have been introduced for requests for images, and these are now controlled through the IG team			
<b>G. ICO Register:</b>				
	1) The content of your registration with the ICO has been reviewed as part of the process for making the required ICO annual payment	In Place		1
<b>H. DPO:</b>				
	1) Provide evidence of notification to the DPO prior to reporting to SLT	In Place		1
	2) Include the DPO's response commentary within the annual report to the SLT	In Place		
	3) Minute the SLT's consideration of the report and any resulting actions	In Place		
<b>I. Consent:</b>				
	1) Consent is only sought for areas where genuine consent is required.	In Place		1
Comments	Mainly just home safety visits and Firebreak. When you telephone home safety, an automated message refers the caller to the privacy notice			
<b>J. Photo &amp; Video:</b>				
	1) Consent for photos and videos is correctly sought and broken down to allow a more informed decision on usage.	In Place		1
<b>K. Marketing:</b>				
	1) There are effective processes in place to ensure that the use of personal data for surveys and marketing purposes is done in compliance with privacy law, including the Privacy of Electronic Communications Regulations (PECR)	In Place		1

### 3. Action Plan

The following areas have been identified as requiring action in order to improve compliance. The Audit Area column below contains the reference to the Audit Area above for which an appropriate control is not in place. Please use the the 3 columns below on the right (headings in grey) to track your progress in resolving this.

Audit Area	Actions Required	Name of Task Owner	Target Date	Completion Date
1. Basic Evidence Pack				
1A1	A DPO role description is in place, though consider amending it using the description provided by IGS (Ref A2 & A3)			
1A2	A member of the SLT or Board would typically undertake the SIRO role, but this role is not currently undertaken by a senior member of staff. It is important to remember that whilst some SIRO duties can be delegated to other members of staff, the responsibility for those duties remains with the SIRO. Ensure there is a role description in place for the SIRO (Ref:A1) and that the role holder is made aware of the requirements of their duties.			
1A3	Ensure the Terms of Reference documents for meetings of Senior Leadership Team / Board includes terms which clarify their responsibilities when making decisions about Information governance issues			
1C1	The Security Measures document should accurately reflect your Technical Security (Ref:H2). This statement should be agreed with your IT support as an accurate representation of how technology is currently managed to keep personal data secure. This should follow a consideration of the risks posed by the current provision and reflect any agreed changes as a result of a risk review. If any issues are identified with current security measures these should be formally recorded as risks on your risk register.			



1C2	<p>The Security Measures document should accurately reflect your Organisational Security (Ref:H2). This should be agreed with any key stakeholders who manage aspects of the measures referred to in the document. This should follow a consideration of the risks posed by the current provision and reflect any agreed changes as a result of a risk review. If any issues are identified with current security measures these should be formally recorded as risks on your risk register.</p>			
1D3	<p>Whilst electronic databases/systems appear to be well managed, with retention built in to them, consider re-organising shared document storage areas (the W Drive) into clear subject structures which are well maintained and where access to sensitive data is controlled. This will improve the authority's overview of where data is held; introduce policy to ensure staff are clear on what information should be stored in the drive and any retention periods that should be adhered to. In addition to electronic data, ensure staff are clear on the retention of hardcopy paper documents, particularly in Stations.</p>			
1E1	<p>Review current privacy notices and ensure all relevant data (ie retention) is included in the notice. Review and publish all relevant service specific privacy notices on your website.</p>			
1E2	<p>Publish the Data Protection Policy Statement which can be found in document ref D2 at Annex C. This should be uploaded to your website alongside your privacy notices.</p>			
1E3	<p>Ensure that the forms you use (paper or digital) to obtain personal data direct the data subjects to the relevant privacy notice(s) which explain the processing.(See statement on document Ref:D2, Annex B)</p>			

1F1	Review the information policies provided by IGS, and ensure that even if you do not adopt the IGS versions, you have equivalent policies in place. Ensure these are in a format that can be easily read and understood by staff.				
1F2	The Authority should make policies available to all staff who handle personal data. Currently staff are informed in a variety of ways when a new policy is issued, but they do not appear to be kept in one specific area where staff can retrieve them easily.				
1F3	Ensure the Data Protection policy and statutory request policy are available on your website, and available to the public.				
1I1	All staff have been asked to complete eLearning provided by Kent F&R, however whilst it has been found that 61% have completed it, ECFRS are unable to determine from them who has not completed it. Suggested they a) contact KFR directly to determine whether this can be provided, if not retrospectively, then going forwards b) Require all staff to complete the training again as it was over a year ago, and request that Team Managers complete reports on when staff have completed the learning, perhaps including this in annual performance reviews. As no certificate is produced, staff could be asked to produce a screen shot of their completion page and provide to managers.				
Audit Area	Actions Required	Name of Task Owner	Target Date	Completion Date	
2. Activity Management					

2A4	Whilst project owners are generally good at ensuring DPIAs are completed when they should be, some departments are still not engaging with IG prior to purchasing new software or engaging new Data Processors. Ensure all departments are made aware of the need to consult the employee responsible for conducting assessments prior to purchasing/appointing and the need to gain approval before proceeding.			
2E2	Ensure NDAs are completed where appropriate (Ref:E6) and are retained in line with records of directly employed staff in order to ensure that complaints received about the individual after they left can be supported for a reasonable period by evidence of the Authority's controls.			
2E3	Establish a process which routinely identifies those who need to sign an NDA when they engage with the Authority and before they gain access to personal data.			
Audit Area	Actions Required	Name of Task Owner	Target Date	Completion Date
3. Review				
3B2	Use the policy change log (document D1) to capture details of policy reviews and maintaining an accurate record over time of what has changed and when			



#### 4. Basis of our Opinion and Assurance Statement

Level	Overall Assurance Rating Description
Good	<b>Good assurance</b> – there is a sound system of internal control designed to achieve the objectives of the system/process and manage the risks to achieving those objectives. Recommendations will normally only be of Low risk rating. Any Moderate recommendations would need to be mitigated by significant strengths elsewhere.
Adequate	<b>Adequate assurance</b> – whilst there is basically a sound system of control, there are some areas of weakness, which may put the system/process objectives at risk. There are Moderate recommendations indicating weaknesses but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any Major recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.

<b>Limited</b>	<b>Limited assurance</b> – there are significant weaknesses in key areas in the systems of control, which put the system/process objectives at risk. There are Major recommendations or a number of moderate recommendations indicating significant failings. Any Critical recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.
<b>No</b>	<b>No assurance</b> – internal controls are generally weak leaving the system/process open to significant error or abuse or reputational damage. There are Critical recommendations indicating major failings

**Auditors' Responsibilities:** 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. Audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses. However, Audit procedures alone, even when carried out with due professional care, do not guarantee that non-compliance will be detected. Accordingly, our examinations as auditors should not be relied upon solely to disclose non-compliant practices, unless we are requested to carry out a special investigation for such activities in a particular area.

Auditor:	Kellene Green	Distribution List:	<b>Releasing Audit Reports:</b> Draft and final reports are retained by Essex County Council for 6 years and only distributed outside the Council's Information Governance Team to the named individuals on the distribution list above. Approval for distributing this report wider should be sought from the relevant Audit sponsor. Care must be taken to protect the control issues identified in this report.
Fieldwork Completed:	13/09/2019	Hope Osayande	
Final Report:	13/09/2019		

Risk Rating	Audit Area Assessment Rationale
 <b>Critical</b>	Major financial loss – Large increase on project budget/cost: (Greater of <b>£1.0M</b> of the total Budget or more than <b>15 to 30%</b> of the organisational budget). Statutory intervention triggered. Impacts the whole Organisation. Cessation of core activities. Strategies not consistent with government's agenda, trends show service is degraded. Failure of major projects – Senior Managers/ Governing bodies are required to intervene. Intense political and media scrutiny i.e. front-page headlines, TV. Possible criminal, or high profile, civil action against the organisation and its employees. Life threatening or multiple serious injuries or prolonged work place stress. Severe impact on morale & service performance. Strike actions etc.
 <b>Major</b>	High financial loss – Significant increase on project budget/cost: (Greater of <b>£0.5M</b> of the total Budget or more than <b>6 to 15%</b> of the organisational budget). Service budgets exceeded. Significant disruption of core activities. Key targets missed, some services compromised. Management action required to overcome medium term difficulties. Scrutiny required by external agencies, Audit Commission etc. Unfavourable external media coverage. Noticeable impact on public opinion.

Serious injuries or stressful experience requiring medical treatment, many workdays lost. Major impact on morale & performance of more than 50 staff



**Moderate**

Medium financial loss – Small increase on project budget/cost: (Greater of **£0.3M** of the total Budget or more than **3 to 6%** of the organisational budget). Handled within the team.

Significant short-term disruption of non-core activities. Standing Orders occasionally not complied with, or services do not fully meet needs. Service action will be required.

Scrutiny required by internal board to prevent escalation. Probable limited unfavourable media coverage.

Injuries or stress level requiring some medical treatment, potentially some workdays lost. Some impact on morale & performance of up to 50 staff.



**Minor**

Minimal financial loss – Minimal effect on project budget/cost: (< **3%** Negligible effect on total Budget or <**1%** of organisational budget)

Minor errors in systems/operations or processes requiring action or minor delay without impact on overall schedule. Handled within normal day to day routines.

Internal review, unlikely to have impact on the corporate image.

Minor injuries or stress with no workdays lost or minimal medical treatment. No impact on staff morale.