Ian Falconer
Partner
T: 0161 953 6480
E: ian.falconer@uk.gt.com

Will Simpson
Senior Manager
T: 0161 953 6486
E: will.g.simpson@uk.gt.com

Fiona Greenbeck
Executive
T: 0161 953 6943
E: fiona.greenbeck@uk.gt.com

Information Commissioner's Office

Internal Audit 2012-13: Civil Monetary Penalties

Last updated 15 March 2013

Distribution		**Timetable**	
For action	Head of Investigations	Fieldwork completed	10 October 2012
For information	Audit Committee	Draft report issued	23 October 2012
	Information Commissioner	Management comments	3 January 2013
	Deputy Commissioner: Data Protection	Final report issued	10 January 2013
	Director of Corporate Services		

Contents

Glossary

The following terms are used in this report:

ICO – Information Commissioner's Office
CIT - Civil Investigations Team
DP – Data Protection
FOI – Freedom of Information
KPI – Key Performance Indicator
PECR – Privacy and Electronic Communications Regulations
RARR – Regulatory Action Recommendation Report

1 Executive Summary

1.1 Background

The Information Commissioner's Office (ICO) is responsible for upholding information rights in the public interest. The Commissioner has the power to impose a Civil Monetary Penalty (CMP) for serious breaches of the Data Protection Act (DPA) or the Privacy and Electronic Communications Regulations (PECR), in addition to his powers to issue undertakings[1] and Enforcement Notices.

The objective of imposing a CMP notice is to promote compliance with both the DPA and the PECR. A serious breach is defined as "a contravention of a kind likely to cause substantial damage or substantial distress".

The ICO has had the power to levy CMPs since April 2010 and, during the year to March 2012, it issued ten penalties for the most serious breaches. As these powers are relatively new and with the aim of continuous improvement, the ICO's processes and procedures continue to evolve to reflect the experiences and periodic review of those involved in the process.

The ICO's Civil Investigation Team (CIT) is responsible for investigating breaches which are reported by data controllers, the public or the media. Once a breach is reported, the ICO will undertake an investigation to determine the full extent and nature of the breach. Data controllers found to have committed breaches may be asked to sign an undertaking, be issued with an enforcement notice, or in the most serious of cases, they may be issued with a CMP.

[1] The culmination of negotiated resolution, an undertaking commits an authority to a particular course of action in order to improve its compliance.

The ICO's Enforcement Department has recently been restructured with the formation of a PECR investigation team and the expansion of the CIT. These changes are intended to allow the CIT to focus on investigating breaches of the DPA.

Please see Appendix A for an outline of the ICO's five stage CMP process.

1.2 Scope

As the ICO has only recently begun enforcement action in relation to CMPs for breaches of the PECR, it was agreed with management that this review would focus on breaches of the DPA. We considered the following sub risks:

- The ICO may not operate a coherent, consistently applied and documented approach to reported breaches of the DPA
- The ICO may not maintain robust records of its investigations into breaches
- The rationale for the CMPs that it issues may not be transparent to both ICO teams and the general public
- The ICO may operate an inefficient approach to investigating cases and issuing CMPs

This audit has been delivered jointly by Grant Thornton UK LLP and the ICO's Good Practice team as part of an initiative to maximise the benefit from their combined assurance resource. Grant Thornton UK LLP retains ownership of the review and responsibility for the opinion provided.

Further details on responsibilities, approach and scope are included in Appendix B.

1.3 Internal Audit Opinion

Design effectiveness	
Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management	**Green**
Operating effectiveness	
Those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review.	**Green**

Refer to Appendix C for definitions of internal audit opinion and recommendation ratings.

1.4 Key findings

Risk	High	Medium	Low	Improve't
The approach to evaluating reported breaches of the DPA	-	1	-	-
The ICO's approach to investigating cases and issuing CMPs	-	2	-	-
The rationale behind CMPs	-	-	-	-
The maintaining of robust records of investigations into breaches	-	-	-	-
Total	**-**	**3**	**-**	**-**

The following findings were rated as medium:

- Following the issuing of several CMPs in high profile cases, and reference to CMPs at workshops, seminars and conferences, the ICO has seen an increase in the number of reported breaches of the DPA. As the level of review work involved in investigating and confirming a serious breach and subsequently issuing a CMP is material, there could be a significantly increased burden on managers. Interim case reviews may also create bottlenecks in the process as Case Officers wait for investigation plans to be approved. Delays also arise in the time it takes data controllers to respond to questions.
As context, between 4% and 5% of cases lead to a CMP. Departmental management needs a clearer understanding of the impact that recent improvements to the CMP process have had on the time taken to complete cases, where and why delays to the completion of cases arise and how these issues can be addressed;
- The CIT aims to complete cases that result in a CMP within an average of 80 working days (112 calendar days). Currently no cases appear to have achieved this target, with some having taken almost a year to conclude. However. new risk based procedures have recently been introduced and cases are being cleared more quickly. The targets for the completion of individual stages should therefore be reviewed, and if they remain appropriate, the resourcing and scheduling implications need to be reconsidered;
- The ICO's aim is to issue CMPs for all breaches where the breach is deemed to be likely to cause substantial damage or distress. The regulatory Action policy sets out the considerations when deciding on issueing a CMP. Due to the volume of breaches reported there is a risk that staff might not view their targets as achievable, and performance, quality and staff morale may suffer. . Management should therefore clearly communicate the rationale for its policy for CMP to the Enforcement team so that they fully understand the team's role.

Further details of our findings and recommendations are provided in Section 2.

1.5 Basis of opinion

We identified the following examples of good practice as part of our review.

Approach to investigating breaches

- There is a clear process in place for documenting how breaches of the DPA are to be investigated. This involves an initial risk based assessment which is completed within 24 hours of a case being received by the Team. The process is communicated to staff through induction and on-going training. Staff have recently received training on investigative interviewing, report writing and negotiation skills.
- Investigation plans are drawn up by Case Officers to document the actions to be undertaken in investigating the breach. These plans are approved by team managers prior to commencing the investigation. Any significant changes to the investigation plan require the plan to be reapproved by the team manager. A review of a sample of investigation plans showed that manager review took place.
- Investigation plans are used to document progress in investigating cases. When the investigation plan is completed it will be reviewed by a team manager who will ensure that sufficient information is available for the case officer to complete a recommendation for regulatory action report.
- A database is used to track the result of finished cases in addition to the use of the case management system.

Rationale for issuing CMPs

- The rationale behind issuing a CMP is documented in the Regulatory Action Recommendation Report (RARR). This includes the details of the breach, an analysis of the available evidence, reviews of the decision and the authorisation of the Head of Enforcement and the Deputy Commissioner – Data Protection.
- The RARR includes a section on the rationale for the penalty which includes a comparison against other penalties levied. All RARRs reviewed included this information.
- The RARR is used by the Enforcement Solicitor to draft a Notice of Intent (NOI); therefore all information required for the ICO to substantiate a penalty must be included in the report. The NOI provides the data controller with the Information Commissioner's preliminary decision and rationale for the proposed CMP and provides them with an opportunity to present any mitigating evidence. The data controller has 28 days to submit representations to the ICO after the NOI has been issued.
- When a final CMP notice is issued the ICO communicates the fact in a press release published on the ICO website. The information communicated by the ICO is agreed with the organisation. All press releases are checked by the case officer for factual accuracy and signed off by either a group manager or the Head of Enforcement.
- Where cases do not progress to a CMP, or any other form of regulatory action, the investigation plan will detail the rationale for the decision. The decision to close a case will be recommended by the case officer and authorised by the team leader to ensure that all cases are appropriately concluded.

Efficiency of the process

- All reported breaches are risk assessed by the Enforcement Department. This is a review of the reported information to allocate a priority to the case; a case will be designated high, medium or low risk. This assessment is undertaken by team managers. Following the risk assessment the highest risk cases will be given priority in allocation to case officers.

1.6 Elsewhere in the sector / Points of interest

We detail below other ways of working and commonly occurring issues that we have experienced during similar types of reviews for other public bodies. The following does not necessarily purport to be good practice but is included for your information and consideration.

- Where cases have taken longer than the target time to complete, there is a requirement to highlight these cases to management in regular reporting, to provide an explanation for the delay and a revised completion date.
- Several organisations break down the KPI for the completion of cases into several stages which each have distinct KPIs and are regularly reviewed to provide early warning of potential delays and in which aspect of the process the delays may be occurring.
- At one organisation, a database is maintained of all completed cases, independent of the case management system which records details of cases and decisions made. This allows those investigating cases and recommending actions to easily review relevant past cases and make consistent recommendations for action. It also provides a useful training tool and supports organisational learning.

1.7 Acknowledgement

We would like to take this opportunity to thank the staff involved in for their co-operation during this internal audit.

2 Detailed Findings

2.1 The ICO may operate an inefficient approach to investigating cases and issuing CMPs resulting in CMPs not being issued in a timely manner and the failure to raise awareness of the implications of serious breaches of data protection to organisations and the general public

1.	Medium	Timeliness and efficiency of process of investigating breaches

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The ICO has robust processes to investigate reported breaches of the DPA which were introduced when it was granted the powers to raise CMPs. As would be expected, over the two years since introduction, the skills and confidence of the CIT have developed along with the tools available for investigating breaches, which have helped improve the efficiency of the CMP process. It is worth noting that the CIT had a change in leadership in December 2011, and has also received additional staff resulting in a recent and necessary restructure. However, due to an increase in the volume of self-reported breaches and the ICO's ability to identify breaches through other means, there has been an increase the number of cases being handled. The level of review involved in processing a serious breach and the issue of a CMP places a significant burden on the workload of case officers and managers and interim manager reviews may create bottlenecks in the process. Case Officers currently have to wait for investigation plans to be reapproved. This therefore identifies a risk that the ICO may not be able to process cases within a timeframe that maximises the	The CIT has concluded a number of CMP cases and has been refining its standard procedures; moving to a risk based approach. The team should continue to review cases to understand the impact that the new approach has had on the time taken to complete cases. This should assist in providing a baseline upon which to build a KPI. It should also consider further how delays in cases being referred to the team from elsewhere within the ICO can be reduced, along with how best to reduce the delays in data controllers responding to investigations. This may involve an evaluation of: • The manager review process; specifically the level (or experience) required and the pool of authority available to sign off each stage. • The time between RARRs being prepared and working group meetings taking place • A review of the current standard documentation (including the template investigation plan) to consider whether	*Casework is continually being reviewed. This includes considering how and where delays occur and ways of streamlining the process. Better ways of monitoring timescales for completion of sections of casework will also be considered.* *The review proces will feed into target setting for 2013/14.* *Date Effective: 31/03/13* *Owner: Stephen Eckersley, Head of Investigations*

1.	Medium	Timeliness and efficiency of process of investigating breaches

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
impact of the penalty using the current process.	these could be refined • Whether there are common documentation sets or investigation requests that are made which could be quickly deployed on acknowledgement of the reported breach, such as a standard request for documentation regarding the data protection controls that are in place. These could reduce duplication of work and shorten the time taken to investigate a breach. • The time taken to investigate each type of breach to ascertain if the workload of case officers is reasonable , and whether the workload of case officers is impacting on the time taken to investigate breaches.	

2.	Medium	Delivery against Key Performance Indicators for concluding cases

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The CIT has a KPI for the processing of CMPs cases of an average of 80 working days (112 calendar days) from when the case is opened to the issue of the NOI on the case. Based on data provided during the review, none of the cases resulting in a CMP under review in 2012-13 had been concluded within this target; indeed the time to complete ranged from 119 days to 357 days. The data also identified that some cases were taking up to 63 days to be allocated to a Case Officer. Explanations for the long time taken to conclude the process include the time taken for Data Controllers to respond to requests for information The CIT has identified projected timescales for each of the five investigation stages, the owner of the stage and the actions involved. Although the team has made changes to the process for investigating self-reported breaches, which have shortened the time frame, from our discussions with staff there is a perception that the KPI is not achievable due to the backlog of cases waiting to be assigned to Case Officers and their current workload. As a result, the KPI is not being used as a tool to motivate Case Officers to achieve the target and to reduce the time taken to process cases.	Building on the above action the ICO should review the KPI for investigating and issuing a CMP to confirm that it is a deliverable target. Management should consider the impact on the KPI of extended response times by data controllers. Recording the proportion of days in the time taken to investigate breaches, will help to understand the reasonableness of the time taken. This review should build upon the work conducted (in recommendation 1 above) to identify and remove bottle necks. It should consider introducing KPIs for the five identified stages of the investigation process to enable management at each level, to identify and address individual problem areas, proactively and on a regular basis. Enforcement Department managers should endorse the use of the agreed KPI to provide motivation to line managers and manage individual performance.	*The KPI for investigating and issuing a CMP will be reviewed in light of the on-going consideration of casework (above).* *Date Effective: 31/03/13* *Owner: Stephen Eckersley, Head of Investigations*

2.2 The ICO may not operate a coherent, consistent and documented approach towards evaluating reported breaches of the DPA resulting in reputation damage to the ICO from the inconsistent treatment of individual cases, the exceeding of the ICO's statutory powers and the potential failure to proceed with breaches that should be considered for a CMP

3.	Medium	Understanding of the importance of fully investigating "most serious" breaches

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The ICO's policy regarding CMPs is to consider issuing CMPs for all breaches which are deemed to be a contravention of a kind likely to cause substantial damage or distress. It also requires cases to be processed in a timely manner to ensure that there is the maximum impact of the penalty being issued. Not all investigations will result in a CMP as the ICO's power to issue a CMP is discretionary, being based on the potential impact of the breach and the results of the investigation. Staff within the CIT commented that although they understood that they should investigate all CMPs that meet the legal criteria, in the context of an increasing workload they did not view it as a deliverable approach. There is therefore a disconnect between staff and management regarding the feasibility of investigating all "most serious" cases with the current resources and the risk that if staff who are responsible for delivering an objective do not view it as achievable and support it, that the objective may not be achieved.	The Executive Team should communicate to the CIT the rationale behind its policy on investigating "most serious" breaches to ensure that the team's role and the overall team objective is clearly understood. Furthermore, the Enforcement management team should inform the CIT of planned actions to improve the efficiency of the CMP process and of the recommended review of targets and KPIs to ensure that they understand that efficiency issues are being considered and addressed.	*The rationale behind the policy on investigating and imposing CMPs is already communicated to the team.* *Staff will be advised of any changes in the CMP process as and when they are made, and of the recommended targets and KPIs; in particular any that arise from the above review.* *Date Effective: 31/03/13* *Owner: Stephen Eckersley, Head of Investigations*

A Outline of CMP process

The CMP process implemented by Enforcement team consists of five distinct stages.

Stage 1 Receive new case	Stage 2 Investigation	Stage 3 First Review	Stage 4 Secondary Investigation	Stage 5 Second Review
• Breach risk assessed by team manager to determine if High, medium or low • Case opened and assigned to case office for investigation - priority given to high risk cases	• Case officer drafts investigation plan • Investigation plan approved by team manager • Investigation undertaken • Amendment to investigation plan approved by team manager • Close Not for Action Cases	• Identify areas requiring clarification and secondary lines of investigation • Identify areas requiring additional ICO support • Check for additional cases • Update IP • Provide IP to line manager for review	• Send and complete secondary lines of enquiry • Obtain responses • Investigation completed • Completed investigation reviewed • Case closed or manager approves case officer to prepare recommendation for regulatory action report (RARR) • Commissioner – Data protection and signed off or returned for re-work accordingly.	• RARR reviewed by case working group - Case working group includes Enforcement Solicitor • Case working group may require additional work to be undertaken by case officer or case working group Or • Case working group agree on recommendation • Case working group meet again to decide on level on penalty • Recommendation of case working group reviewed by Head of Enforcement • Commissioner – Data protection reviews the recommendation report and signs off or returns for re-work. Notice of intent prepared by Enforcement Solicitor • Notice of Intent signed off by Deputy Commissioner • Notice of Intent issued
Actions following issuing of Notice of Intent. • Representations received from organisation. • Representations considered • Relevant actions taken • Civil Monetary Penalty issued **Post closure processes** These include, Lessons learnt, QA Process, Reporting of outputs, Feedback on team performance, Service compliments, complaints and case review requests				

B Internal audit approach

Approach

Our audit was carried out in accordance with the guidance contained within the Government's Internal Audit Standards and the Auditing Practices Board's 'Guidance for Internal Auditors'. We also had regard to the Institute of Internal Auditors' guidance on risk based internal auditing (2005).

Our internal audit approach is based upon the underlying principles of the UK Corporate Governance Code (2010) together with the associated Turnbull Committee guidelines on internal control (2005) that require management to identify, assess and manage the risks that are significant to the achievement of the organisation's overall business objectives. We will also have regard to the HM Treasury Management of Risk Guidance (2001). Our role as internal auditor is to provide objective and independent assurance to the Audit Committee and management that it is doing so successfully for each of the areas being audited.

As part of our 2012-13 Audit Plan, we agreed with the Audit Committee and management that we should carry out a review of the ICO's arrangements for managing Civil Monetary Penalties to improve our on-going understanding of the ICO's key internal control activities..

We achieved our audit objectives by:

- agreeing the principles and benefits of effective risk management arrangements with management;
- meeting with key staff to gain an understanding of the arrangements in place, building upon the information we have already gained through our audit planning process;
- reviewing key documents that support the processes in place; and
- comparing existing arrangements with established best practice and other guidance.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of internal control arrangements.

Scope

This audit has been delivered jointly by Grant Thornton UK LLP and the ICO's Good Practice team as part of an initiative to maximise the benefit from their combined assurance resource. Grant Thornton UK LLP retains ownership of the review and responsibility for the opinion provided.

Our review focused on the following risks:

- The ICO may not operate a coherent, consistent and documented approach towards evaluating reported breaches of the DPA resulting in reputation damage to the ICO from the inconsistent treatment of individual cases, the exceeding of the ICO's statutory powers and the potential failure to proceed with breaches that should be considered for a CMP. The rationale behind the CMPs that are issued may not be transparent to both ICO teams and the general public resulting in inconsistencies between the nature and seriousness of breaches and the value of CMPs issued and the increase in costly and time consuming appeals to decisions made by the ICO
- The ICO may not maintain robust records of investigations into breaches that may result in CMPs resulting in a failure to substantiate how and why CMPs have been determined and a failure to learn lessons from earlier cases and inconsistencies in the nature and value of CMPs issued

- The ICO may operate an inefficient approach to investigating cases and issuing CMPs resulting in CMPs not being issued in a timely manner and the failure to raise awareness of the implications of serious breaches of data protection to organisations and the general public.

The ICO's approach for receiving reports of breaches which lead to CMPs is deemed to be outside of the scope of this review.

Additional information

Client staff

The following staff were consulted as part of this review:

- David Smith – Deputy Information commissioner - DP
- Simon Entwisle – Head of Operations
- Stephen Eckersley – Head of Enforcement
- Sally-Anne Poole – Enforcement Group Manager
- Andy Curry – Enforcement Group Manager
- Joanne Stones - Team Manager, Enforcement (Civil Investigation Team)
- Cathy Devitt – Enforcement Solicitor
- Daniela Guadagno. Lead Case Officer, Enforcement
- Andrew Powell – Enforcement Case Officer

Locations

The following locations were visited during the course of this review:

- The Information Commissioner's Office, Wilmslow.

C Definition of internal audit opinion and ratings

Internal audit opinion

Design effectiveness	Opinion	Operating effectiveness	Rating
We have not been able to form an opinion on whether the internal controls examined have been designed to achieve the risk management objectives required by management	No opinion can be given	We have not been able to form an opinion on whether the internal controls examined were operating to provide reasonable assurance that the related risk management objectives were achieved during the period under review	No opinion can be given
Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management	Green	Those activities and controls were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review	Green
Overall, we have concluded that, except for the specific weaknesses identified by our audit, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management.	Amber	Except for the controls listed below those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review.	Amber
Overall, we have concluded that, in the areas examined, the risk management activities and controls are not suitably designed to achieve the risk management objectives required by management.	Red	Those activities and controls that we examined were not operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review	Red

Audit issue rating

Within each report, every audit issue is given a rating. The ratings are summarised in the table below.

Rating	Description	Features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	• Key control not designed or operating effectively • Potential for fraud identified • Non compliance with key procedures / standards • Non compliance with regulation
Medium	Important findings that are to be resolved by line management.	• Impact is contained within the department and compensating controls would detect errors • Possibility for fraud exists • Control failures identified but not in key controls • Non compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures.	• Minor control weakness • Minor non compliance with procedures / standards
Improvement	Items requiring no action but which may be of interest to management or best practice advice	• Information for department management • Control operating but not necessarily in accordance with best practice

www.grant-thornton.co.uk